METHOD FOR CONDUCTING TRANSACTIONS

Publication number: RU2157001
Publication date: 2000-09-27
Inventor: ZOLOTAREV O A; KUZNETSOV I V; MOSHONKIN A G; SMIRNOV A L; KHAMITOV I M
Applicant: ALKORSOFT AOZT
Classification:
- international: ***G06Q10/00; G06Q20/00; G06Q30/00; G07F7/10; G09C1/00;*** **G06Q10/00; G06Q20/00; G06Q30/00; G07F7/10; G09C1/00;** (IPC1-7): G07F19/00; G06F17/60; G07D7/00
- European: G06Q20/00K1; G06Q20/00K2B; G07F7/10E
Application number: RU19980120922 19981125
Priority number(s): RU19980120922 19981125

Also published as:
EP1134708 (A1)
WO0031700 (A1)
US6859795 (B1)
CA2351588 (A1)
AU770762B (B2)

Report a data error here

Abstract of **RU2157001**

sale systems, electronic mass service systems, communication equipment. SUBSTANCE: Device may be used exchange of securities, organization of payment systems and sale systems using computer networks, organization of banks and bank systems, shops, service centers, lotteries, and so on. The method involves choosing payment secret and public keys, running accumulation transactions, preparation of payment certificate basis, production and addition of payment request, generation of payment signature, checking payment solvency of certificate, adding public key into basis of payment certificate, adding data about payment receiver, payment conditions and identifier of used payment certificate into payment order, selection of secret key of account signature, linking it to open account, generation of signature of payment order of receiver, and processing data about commitment of receiver. EFFECT: protection of financial interests of each participants against breach of confidence by other partners, protection of privacy of payers and receivers of payments. 109 cl, 14 ex

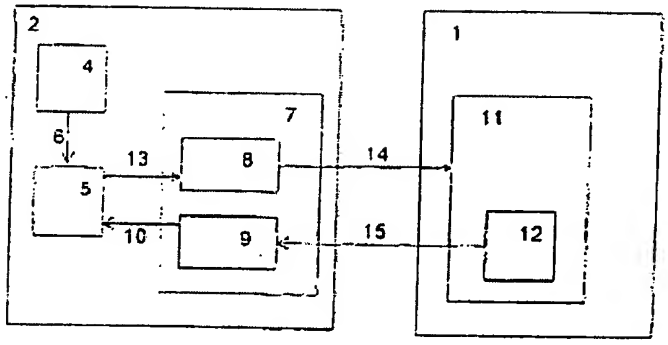

Fig. 2

(19) **RU** (11) **2 157 001** (13) **C2**

(51) МПК[7] **G 07 F 19/00, G 06 F 17/60, G 07 D 7/00**

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21), (22) Заявка: 98120922/09, 25.11.1998

(24) Дата начала действия патента: 25.11.1998

(46) Дата публикации: 27.09.2000

(56) Ссылки: D. CHAUM, SECURITY WITHOUT IDENTIFICATION: TRANSACTION SYSTEMS TO MAKE BIG BROTHER OBSOLETE, COMMUNICATIONS OF THE ACM, vol.28 no 10, OCTOBER 1985, p.1030-1044. RU 2022351 C1, 30.10.1994. US 4977595 A, 11.12.1990. US 5768385 A, 16.06.1998. US 5224162 A, 29.06.1993. RU 2094846 C1, 27.10.1997. RU 2096826 C1, 20.11.1997.

(98) Адрес для переписки:
199034, Санкт-Петербург, Университетская наб. 7/9, Университет, Межвузовский патентно-лицензионный отдел, Матвеевой Т.И.

(71) Заявитель:
Закрытое акционерное общество "Алкорсофт"

(72) Изобретатель: Золотарев О.А., Кузнецов И.В., Мошонкин А.Г., Смирнов А.Л., Хамитов И.М.

(73) Патентообладатель:
Закрытое акционерное общество "Алкорсофт"

(54) СПОСОБ ПРОВЕДЕНИЯ ПЛАТЕЖЕЙ (ВАРИАНТЫ)

(57)

Изобретение относится к торговым системам, электронным системам массового обслуживания, платежным системам, коммуникационным системам и может быть использовано для организации торговли ценными бумагами, для организации платежных систем и систем торговли на основе компьютерных сетей, для организации банков и банковских систем, магазинов, сервисных центров, лотерей и т.п. Техническим результатом является то, что при проведении платежей по открытым телекоммуникационным сетям обеспечивается защита денежных интересов каждого участника от злоупотреблений других участников, обеспечивается защита приватности плательщиков и получателей. Способ проведения платежей заключается в том, что выбирают денежные секретные и открытые ключи, проводят операции пополнения, создают основу платежного сертификата, формируют и добавляют денежный запрос, создают денежную подпись, проверяют правильность изготовления подписи денежного сертификата, проверяют платежеспособности сертификата, включают в основу платежного сертификата открытый ключ, включают в платежное поручение плательщика сведения о получателе платежа, условия платежа, идентификатор используемого платежного сертификата, выбирают секретный ключ подписи счета, связывают его с открытым счетом, изготавливают подпись платежного поручения получателя, производят обработку данных обязательств получателя. 7 с. и 102 з.п. ф-лы.

RU 2157001 C2

RU 2157001 C2

(19) **RU** (11) **2 157 001** (13) **C2**

(51) Int. Cl.[7] **G 07 F 19/00, G 06 F 17/60, G 07 D 7/00**

RUSSIAN AGENCY
FOR PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: 98120922/09, 25.11.1998

(24) Effective date for property rights: 25.11.1998

(46) Date of publication: 27.09.2000

(98) Mail address:
199034, Sankt-Peterburg, Universitetskaja nab. 7/9, Universitet, Mezhvuzovskij patentno-litsenzionnyj otdel, Matveevoj T.I.

(71) Applicant:
Zakrytoe aktsionernoe obshchestvo "Alkorsoft"

(72) Inventor: Zolotarev O.A., Kuznetsov I.V., Moshonkin A.G., Smirnov A.L., Khamitov I.M.

(73) Proprietor:
Zakrytoe aktsionernoe obshchestvo "Alkorsoft"

(54) METHOD FOR CONDUCTING TRANSACTIONS

(57) Abstract:

FIELD: sale systems, electronic mass service systems, communication equipment. SUBSTANCE: Device may be used exchange of securities, organization of payment systems and sale systems using computer networks, organization of banks and bank systems, shops, service centers, lotteries, and so on. The method involves choosing payment secret and public keys, running accumulation transactions, preparation of payment certificate basis, production and addition of payment request, generation of payment signature, checking payment solvency of certificate, adding public key into basis of payment certificate, adding data about payment receiver, payment conditions and identifier of used payment certificate into payment order, selection of secret key of account signature, linking it to open account, generation of signature of payment order of receiver, and processing data about commitment of receiver. EFFECT: protection of financial interests of each participants against breach of confidence by other partners, protection of privacy of payers and receivers of payments. 109 cl, 14 ex

RU 2157001 C2

RU 2157001 C2

Изобретение относится к области электронных платежных систем, торговых систем, электронных систем массового обслуживания и коммуникационных систем и может быть использовано для организации банков и банковских систем, магазинов, сервисных центров, торговли ценными бумагами, лотерей и т.п.

Электронные платежные системы предназначены для проведения сделок по коммуникационным сетям. Помимо безопасности, надежности, стоимости обслуживания, быстродействия и т. п. важной характеристикой платежной системы является защита приватности пользователей. Приватность пользователя предполагает, что никто, в том числе и оператор платежной системы, не в состоянии контролировать покупки пользователя. Один из способов защиты приватности в электронных платежных системах состоит в том, что покупки совершают с помощью цифровых данных, которые подтверждают платежеспособность, но не ведут к идентификации личности плательщика. Однако, такие данные, как и любые цифровые данные, легко копируются, что требует заботы о предотвращении их многократного использования.

Известен способ проведения платежей (T. Okamoto, K. Ohta, Electronic cash system, U.S. Patent 5,224,162, 8 Jun 1992), в котором плательщик получает в банке посредством операции изготовления вслепую цифровой подписи данные для изготовления платежных сертификатов, которые содержат в скрытой форме идентификатор плательщика и которыми он расплачивается с другими участниками платежной системы. При этом защита от кратного использования платежных сертификатов обеспечивается тем, что идентификатор плательщика, допустившего кратное использование, может быть раскрыт. Однако этот способ не обеспечивает предотвращения кратного использования, так как безопасность банка и иных участников платежной системы зависит от поведения третьих лиц.

Далее приведено пояснение используемых понятий. Под платежным сертификатом имеются в виду цифровые данные, представляющие обязательство оператора платежной системы. Платежный сертификат включает цифровую подпись оператора платежной системы, подтверждающую номинальную стоимость сертификата и называемую подписью платежного сертификата.

Цифровая подпись, также называемая для краткости просто подписью, широко используется на практике и играет роль, аналогичную роли обычной рукописной подписи. Однако цифровая подпись имеет те преимущества, что ее достоверность легко проверяема, ее подделка весьма затруднительна, она легко может быть передана по телекоммуникационным каналам. Цифровая подпись для некоторых исходных данных представляет собой другие данные, удовлетворяющие заранее оговоренному свойству цифровой подписи. Под данными понимается произвольная информация, которая может быть представлена в цифровой форме. При этом данные могут быть представлены и в других формах, а также могут быть перекодированы из одной формы в другую.

Для изготовления цифровой подписи подписывающая сторона выбирает секретную функцию и соответствующую ей проверяющую функцию. Для изготовления цифровой подписи на исходных данных податель, то есть субъект, желающий получить цифровую подпись, передает их подписывающей стороне, которая изготавливает цифровую подпись с помощью обработки исходных данных секретной функцией и передает изготовленную подпись подателю. Как податель, так и любая иная сторона с помощью общеизвестной проверяющей функции может проверить, удовлетворяют ли полученная от подписывающей стороны цифровая подпись свойству подписи для исходных данных. Под секретным ключом подписи понимаются данные, которые позволяют изготавливать цифровую подпись, а под соответствующим секретному ключу открытым ключом понимаются данные, которые позволяют проверять правильность цифровой подписи. Секретные и соответствующие им открытые ключи создают с помощью соответствующих устройств, называемых генераторами ключей. Описание многочисленных примеров цифровой подписи, а также соответствующих генераторов ключей, подписывающих устройств и устройств для проверки подписи, обычно реализуемых на основе запрограммированных компьютеров, имеется в книгах: B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley&Sons, New York, 2nd edition, 1996 и A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997. Генераторы ключей могут включать датчики случайных чисел, то есть устройства, на выходе которых появляются данные подходящей разрядности, предпочтительно непредсказуемые для стороны, неконтролирующей работу такого устройства. Такие устройства хорошо известны. В частности, в качестве датчиков случайных чисел могут использоваться датчики "псевдослучайных" чисел. Помимо цифровой подписи открытые ключи могут применяться для шифрования сообщений на имя владельца соответствующего секретного ключа, который с помощью этого секретного ключа может расшифровывать такие сообщения. Открытые и секретные ключи, предназначенные для этих целей, называются открытыми и секретными ключами для шифрования.

В некоторых приложениях для защиты приватности подателя желательно, чтобы цифровая подпись изготавливалась вслепую. Это название происходит от того, что подписывающая сторона в ходе изготовления цифровой подписи не получает информации об исходных данных и, тем самым, не видит то, что она подписывает. Фактически под изготовлением вслепую цифровой подписи понимается такое изготовление подписи, при котором обеспечивается непрослеживаемость, означающая, что для подписывающей стороны, которая получит впоследствии подписи многих исходных данных, будут в достаточной мере равновероятны возможные соответствия между этими подписями и обработанными

RU 2157001 C2

RU 2157001 C2

замаскированными данными.

Непрослеживаемость обеспечивается тем, что множество всех замаскированных данных, созданных на основе одних выбранных исходных данных совпадает с аналогичным множеством для других случайно выбранных исходных данных. Разумеется, что на практике достаточно обеспечить достаточно малую вероятность несовпадения вышеуказанных множеств. Таким образом, сказать, что способ изготовления подписи обеспечивает непрослеживаемость, то же самое, что и назвать такой способ способом изготовления подписи вслепую.

Общий метод изготовления вслепую цифровой подписи для некоторых исходных данных состоит в том, что податель создает на основе исходных данных и маскировочного ключа, который может быть назван ослепляющим ключом, замаскированные данные, которые также могут быть названы ослепленными. Замаскированные данные предоставляет подписывающей стороне в качестве данных для изготовления вслепую подписи, а подписывающая сторона возвращает подателю в качестве результата обработки данных для изготовления вслепую подписи данные для демаскировки. После этого податель завершает изготовление вслепую цифровой подписи для исходных данных, производя демаскировку результата обработки замаскированных данных. Такая демаскировка может производиться с помощью демаскирующего устройства, которое может быть, в частности, реализовано компьютером, запрограммированным в соответствии с используемой схемой изготовления вслепую цифровой подписи.

Известны многочисленные способы изготовления цифровой подписи вслепую (D. Chaum, Blind Signature Systems, U.S. Patent 4,759,063, 19 Jul 1988; B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley& Sons, New York, 2nd edition, 1996; A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997). К таким способам относятся, в частности, и способы изготовления вслепую цифровой подписи, обладающие дополнительными свойствами (например, D. Chaum, Blind Unanticipated Signature Systems, U.S. Patent 4,759,064, 19 Jul 1988). Другие способы изготовления цифровой подписи вслепую описаны, например, в D. Pointcheval, J. Stern, Provably Secure Blind Signature, Lectures Notes in Computer Science, 1163, 1996, Springer, p. 252-265.

Известен способ проведения платежей (D. N. Simon, Untraceble electronic cash, U. S. Patent 5,768,385, 16 Jun 1998), в котором плательщик получает в банке цифровые подписи платежных сертификатов, называемых электронными монетами, которые он может использовать как для обмена на новые электронные монеты, так и для платежа. При этом банк не знает в каком из этих двух режимов действует плательщик, что способствует непрослеживаемости платежей. При этом защита от кратного использования электронных монет обеспечивается онлайновой проверкой получателем платежа полученных электронных монет в банке. Однако известный способ не обеспечивает полной непрослеживаемости такого участника системы, который в основном платит, а не получает платежи, так как электронные монеты, выданные такому участнику и предъявленные магазином для обмена, свидетельствуют, вообще говоря, о проведении платежа данным участником данному магазину.

Известен способ проведения платежей (D. Chaum, Security Without Identification: Transaction Systems to Make Big Brother Obsolete, Communications of the ACM, vol. 28 no. 10, October 1985 pp. 1030-1044), который является наиболее близким аналогом к предлагаемому изобретению и выбран в качестве прототипа. В этом способе плательщик расплачивается платежными сертификатами, называемыми электронными монетами, подписи которых он получает в банке. При этом заранее фиксируется набор возможных номиналов, а для каждого возможного номинала электронной монеты банк создает денежные секретный и открытый ключи, то есть ключи для изготовления и проверки подписи, удостоверяющей ценность платежных сертификатов. Для получения электронной монеты плательщик выбирает ее номер посредством датчика случайных чисел и с помощью процедуры изготовления вслепую цифровой подписи в банке, желающем прокредитовать плательщика на соответствующую сумму, получает в качестве подписи платежного сертификата цифровую подпись выбранного номера. При платеже плательщик передает получателю набор электронных монет, а получатель, проверив их правильность, пересылает полученные монеты в банк для зачисления на свой счет. Банк, проверив правильность электронных монет, зачисляет соответствующую сумму на счет получателя платежа, если монеты не были использованы ранее. Для проверки использованности банк хранит список номеров использованных монет, причем встроенные в номера монет сроки действия позволяют удалять из списка старые номера.

Недостатки известного способа состоят в том, что деньги клиента не защищены от нечестного банка, а репутация банка не защищена от нечестных клиентов, так как получив сертификат на проверку, нечестный банк может заявить, что этот сертификат уже предъявлялся ранее. В свою очередь, нечестный клиент, получив отказ банка признать уже использованный сертификат второй раз, может обвинить банк в нечестности. Кроме того, банк вынужден хранить в оперативных базах данных информацию о каждом из использованных сертификатов, что приводит к быстрому росту баз данных банка и к необходимости введения временных ограничений на действие сертификатов. Помимо этого, в известном способе сумма платежа является целочисленной комбинацией номиналов монет, что либо ограничивает диапазон платежей, либо ведет к росту числа используемых при платежах монет, что ведет к росту баз данных в банке и замедлению платежей.

Недостатки прототипа устраняются предложенными вариантами способа проведения платежей. Основной задачей, решаемой вариантами данного изобретения,

RU 2157001 C2

RU 2157001 C2

является создание таких способов проведения платежей, которые обеспечили бы эффективный и надежный механизм расплаты по открытым коммуникационным сетям, защиту каждого участника платежной системы от злоупотреблений всех других участников, защиту приватности рядовых участников платежей, широкий диапазон платежей.

Единый для всех вариантов данного изобретения технический результат состоит в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности. Помимо этого, в некоторых вариантах доступны платежи в диапазоне от микроплатежей до платежей бизнес-уровня, время проведения платежа зависит только от быстроты действия сетевых соединений, но не от суммы платежа, число клиентов, которые могут быть обслужены оператором платежной системы, растет пропорционально его ресурсам. Помимо этого, в некоторых вариантах допускаются постепенное расходование платежных сертификатов и их пополнение.

Существенное отличие данного изобретения от известного уровня техники и прототипа заключается в том, что помимо защиты приватности участников платежа обеспечена защита денежных интересов плательщика тем, что платеж проводится на основании его платежного поручения, подписанного связанным с платежным сертификатом секретным ключом.

Перед описанием сущности изобретения поясним используемую терминологию. Под оператором платежной системы имеется в виду субъект, обеспечивающий проведение расчетов участников платежной системы. В частности оператор платежной системы может вести счета участников платежей и эмитировать ценные документы. Оператор платежной системы может состоять из одного банка, а может включать в себя несколько организаций, в том числе и банков, которые связаны между собой различными договорными обязательствами. В частности, секретные ключи оператора платежной системы могут быть секретом одной из организаций, входящих в состав оператора платежной системы, а обязательства оператора платежной системы перед третьей стороной также могут быть обязательствами лишь одной из организаций, входящих в состав оператора платежной системы. В случае, если оператор платежной системы включает несколько платежных серверов, то есть устройств для обслуживания участников платежной системы, принадлежащих различным банкам или иным организациям, должна иметься безопасная система урегулирования взаимных обязательств между организациями, входящими в состав оператора платежной системы. Такие безопасные системы урегулирования взаимных обязательств известны специалистам.

Используемые при реализации данного изобретения платежные сертификаты включают данные, называемые основой платежного сертификата. При этом подпись платежного сертификата, подтверждающая номинальную стоимость сертификата, является подписью оператора платежной системы для этой основы. Под номером основы имеются в виду данные, идентифицирующие основу. Под авторизацией платежного сертификата имеется в виду процедура признания эмитентом платежного сертификата своих обязательств по нему. Данная процедура может включать проверку эмитентом подписи авторизуемого сертификата, проверку срока годности и иных данных. В некоторых схемах цифровой подписи легко изготовить подпись для случайных данных без знания секретных ключей подписи. Поэтому для защиты оператора платежной системы от подделок подписи среди всех основ платежных сертификатов выделяют множество действительных основ или, иными словами, выбирают критерий действительности основ платежных сертификатов.

Под данными обязательства получателя платежа перед плательщиком имеются в виду данные, представляющие собой описание тех обязательств, которые берет на себя получатель платежа в случае его проведения.

Плательщик проводит свои операции с помощью платежного устройства, которое может быть реализовано различными способами, в частности, как в виде специализированного устройства, так и на основе соответствующим образом запрограммированного компьютера.

Указанный выше технический результат при реализации изобретения достигается тем, что способ проведения платежей по первому варианту, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одну основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего изготавливают подпись платежного сертификата введением доставленных данных для демаскировки в демаскирующее устройство и осуществляют проверку правильности изготовленной подписи платежного сертификата введением ее и денежного открытого ключа, соответствующего использованному оператором платежной системы денежному

RU 2157001 C2

RU 2157001 C2

секретному ключу, в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, причем при проверке платежеспособности используемого при платеже платежного сертификата оператор платежной системы проводит операцию его авторизации, при которой по наличию информации об авторизуемом платежном сертификате в информационном хранилище отказывают в авторизации, а по ее отсутствию осуществляют проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, и в случае правильности заносят информацию об авторизуемом платежном сертификате в информационное хранилище, после чего формируют ответ оператора платежной системы на платежное поручение получателя платежа и доставляют его посредством коммуникационных сетей получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, отличается тем, что в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи платежного сертификата посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа посредством генератора ключей выбирает секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством введения его и секретного ключа подписи счета получателя платежа в подписывающее устройство, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, в информационное хранилище при авторизации платежного сертификата заносят подписанное платежное поручение плательщика, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которой судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

Указанный выше технический результат в частных случаях конкретной реализации может достигаться, кроме того, тем, что при создании основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификата и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией. В частности, при включении в основу платежного сертификата идентификатора открытого ключа подписи

RU 2157001 C2

RU 2157001 C2

платежного сертификата, в качестве этого идентификатора может быть использован сам открытый ключ подписи платежного сертификата. Помимо этого, при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата может быть включен в основу в качестве дополнительного номера.

Кроме того, перед включением в платежные данные платежного поручения плательщика оно может быть зашифровано одним из открытых ключей для шифрования оператора платежной системы. В этом случае оператор платежной системы дешифрует полученное от получателя платежа платежное поручение плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования. Более того, оператор платежной системы может осуществлять шифрование своего ответа на платежное поручение получателя платежа.

Кроме того, в условия платежа, содержащиеся в платежном поручении плательщика, могут быть включены данные обязательства получателя платежа перед плательщиком. Более того, при подготовке плательщиком платежных данных данные обязательства получателя платежа перед плательщиком могут быть обработаны наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включены в подготавливаемое платежное поручение плательщика, причем получатель платежа также производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа. В частности, наперед заданная маскирующая функция может быть выбрана произвольно из множества односторонних функций.

Помимо этого, получатель платежа может подписать данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей подписи и до платежной операции проверить подпись получателя платежа для данных обязательства получателя платежа перед плательщиком.

В частности, при проведении операции пополнения платежного устройства в качестве источника кредитования может быть использован счет плательщика, который предварительно кредитуют при платежной операции. Помимо этого, при проведении операции пополнения платежного устройства в качестве источника кредитования может быть использована банковская карточка.

Помимо этого, при проведении платежной операции в качестве плательщика может выступать получатель платежа, а оператор платежной системы может иметь несколько платежных серверов.

Ниже приведены примеры частных случаев реализации как отдельных операций, так и изобретения в целом. В примерах 1 и 2 приведены два частных случая критерия действительности основ платежных сертификатов.

Пример 1

Основа платежного сертификата представляет последовательность битов достаточно большой длины, причем основа считается действительной, если все нечетные биты этой последовательности равны нулю.

Пример 2

Основа платежного сертификата представлена двумя последовательностями битов X и Y, причем данные X выступают в качестве номера основы, данные Y выступают в качестве дополнительного номера, а основа считается действительной, если f(Y) = X, где функция f является односторонней, то есть, в данном случае, вычислительно необратимой для всех, кроме, возможно, оператора платежной системы.

Под односторонней функцией понимается преобразование данных, которое в вычислительном смысле практически необратимо. Известны многочисленные примеры таких функций и их вычислителей, то есть средств для вычисления таких функций, реализуемых часто с помощью соответствующим образом запрограммированного компьютера (B. Schneier, Applied CryptograpHy: Protocols, Algorithms, and Source Code in C, John Wiley &Sons, New York, 2nd edition, 1996; A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997). Широкий класс односторонних функции представляют так называемые хэш-функции. При этом, в зависимости от цели использования, на односторонние функции накладывают дополнительные требования, такие, например, как практическая невозможность найти два значения, имеющих один и тот же образ при односторонней функции. Такие односторонние функции иногда называют односторонними функциями без столкновений. Также к классу односторонних функций принадлежат односторонние функции с "лазейкой". При этом такие функции не удовлетворяют требованию односторонности для стороны, владеющей некоторым секретом ("лазейкой"), позволяющим, например, обращать одностороннюю функцию. Тем не менее, если защита безопасности стороны, опубликовавшей такую функцию, основана на предположении, что для сторон, не владеющих "лазейкой", опубликованная функция является односторонней, то такую функцию также следует рассматривать как одностороннюю.

Для некоторых схем подписи, в частности для RSA-подписи, легко получить подпись под некоторыми случайными данными без знания соответствующего секретного ключа. Для предотвращения такой возможности в некоторых схемах цифровой подписи подписывающая сторона объявляет подпись правильной только в том случае, если в подлежащие подписи данные встроен образ односторонней функции от некоторого известного получателю подписи значения. В этом случае односторонняя функция предназначена для защиты подписывающей стороны и может иметь "лазейку", являющуюся секретом подписывающей стороны.

Кроме того, односторонние функции могут использоваться для идентификации данных без их раскрытия. Например, если сторона, контролирующая идентичность некоторых данных X и Y владеет только их образами при односторонней функции, которая является

RU 2157001 C2

RU 2157001 C2

односторонней функцией без столкновений, а сами данные X и Y не доступны для контролирующей стороны, то эта сторона может сделать вывод, что совпадают и сами данные X и Y.

Имеется в виду, что цифровая подпись основы платежного сертификата может быть представлена другой цифровой подписью для части данных, входящих в основу, при условии, что имеется связь этой части данных с остальными данными основы. Например, в примере 2 цифровая подпись для основы (X,Y) может быть представлена некоторой цифровой подписью для данных X и данными Y, а при проверке правильности подписи основы, кроме проверки правильности подписи для X, проверяют и соотношение f(Y) = X.

Сущность способа проведения платежей по первому варианту состоит в том, что оператор платежной системы выбирает денежные секретные ключи и соответствующие денежные открытые ключи в рамках некоторой схемы цифровой подписи, допускающей изготовление цифровой подписи вслепую. Каждой паре из денежных открытого и соответствующего секретного ключей ставится в соответствие определенная номинальная стоимость, причем денежные открытые ключи и соответствующие им номинальные стоимости публикуются.

Для пополнения своего платежного устройства плательщик выбирает секретный ключ подписи платежного сертификата и соответствующий ему открытый ключ подписи платежного сертификата в рамках некоторой системы цифровой подписи, выбирает основу платежного сертификата, включающую его номер и идентификатор открытого ключа подписи платежного сертификата, после чего производит маскировку номера платежного сертификата в рамках некоторой схемы изготовления вслепую цифровой подписи и доставляет оператору платежной системы денежный запрос, включающий замаскированный номер, указание на источник кредитования и, возможно, сумму кредитования, если она не предусмотрена иными обстоятельствами, например условиями обслуживания указанного источника кредитования. Например, в качестве источника кредитования может быть указан счет плательщика или его банковская карточка. Безопасность удаленного востребования ценностей с указанного источника кредитования должна быть обеспечена системой обслуживания этого источника кредитования.

Получив денежный запрос, оператор платежной системы по этому запросу определяет источник и сумму кредитования, выбирает денежный секретный ключ, соответствующий сумме кредитования, изготавливает данные для демаскировки, по которым плательщик может изготовить подпись платежного сертификата и доставляет изготовленные данные для демаскировки плательщику. При этом платежеспособность источника кредитования уменьшается в соответствии с суммой кредитования и стоимостью данной услуги оператора платежной системы.

Получив от оператора платежной системы данные для демаскировки, плательщик изготавливает подпись платежного сертификата демаскировкой полученных данных и получает тем самым годный для проведения платежной операции платежный сертификат. Приватность плательщика обеспечена тем, что подпись платежного сертификата изготовлена вслепую и, тем самым, прервана ее связь с источником кредитования.

Для получения платежа получатель открывает у оператора платежной системы счет, допускающий безопасное удаленное управление. Для этого получатель платежа выбирает секретный ключ подписи счета и соответствующий открытый ключ подписи счета в рамках некоторой схемы цифровой подписи и доставляет открытый ключ подписи счета оператору платежной системы, который открывает счет и связывает его с полученным открытым ключом подписи счета. В дальнейшем оператор платежной системы проводит операции с данным счетом, руководствуясь подписанными указаниями, подпись для которых изготавливается владельцем счета с помощью секретного ключа подписи счета и проверяется оператором платежной системы с помощью открытого ключа подписи счета. Безопасность владельца счета обеспечивается тем, что оператор платежной системы отчитывается перед владельцем счета подписанными указаниями. Для удобства счету может быть присвоен номер, который сообщается владельцу счета. Субъект, открывающий счет у оператора платежной системы, считает счет открытым только после получения подписанного оператором платежной системы сообщения, которое подтверждает открытие счета, связанного с открытым ключом подписи счета.

Плательщик, имея годный платежный сертификат и желая заплатить получателю платежа соответствующую стоимость, готовит платежные данные, включающие предназначенное для оператора платежной системы платежное поручение плательщика и, возможно, данные, предназначенные для получателя платежа. Данные, предназначенные для получателя платежа, могут включать указание услуги или товара, которые оплачивает плательщик. В платежное поручение плательщика включают основу платежного сертификата, сведения о получателе платежа, в частности идентификатор счета получателя платежа, если этот счет не определен иными обстоятельствами, и условия платежа. Условия платежа могут содержать, возможно в скрытой с помощью обработки маскирующей функцией от оператора платежной системы форме, обязательства, накладываемые на получателя платежа фактом его проведения. При этом платежное поручение плательщика подписывается секретным ключом подписи платежного сертификата. Подготовленные платежные данные доставляют получателю платежа.

Получатель платежа, желая принять платеж, формирует свое платежное поручение, включающее полученное платежное поручение плательщика и условия платежа, подписывает его секретным ключом подписи того счета, на который он принимает платеж, и доставляет оператору платежной системы.

RU 2157001 C2

RU 2157001 C2

Оператор платежной системы при наличии записи о платежном сертификате, основа которого содержится в платежном поручении плательщика, в поддерживаемом им списке использованных платежных сертификатов, считает данный платежный сертификат использованным и отказывает в его авторизации. Платеж также не проводится, если не верна подпись платежного поручения плательщика, проверяемая содержащимся в присланной основе платежного сертификата открытым ключом подписи, или не верна подпись для полученного платежного поручения получателя платежа, проверяемая открытым ключом подписи счета получателя платежа, а также если условия платежа, содержащихся в платежных поручениях плательщика и получателя платежа, не соответствуют друг другу. Если же все эти условия проведения платежа выполнены, то оператор платежной системы, проверив правильность подписи платежного сертификата, заносит в список использованных платежных сертификатов сведения о данном платежном сертификате вместе с подписанным платежным поручением плательщика, кредитует на соответствующую номинальной стоимости сумму счет получателя платежа, сохранив при этом подписанное поручение получателя платежа, и доставляет получателю платежа ответ оператора платежной системы на платежное поручение получателя платежа, включающий подписанную оператором платежной системы квитанцию получателя платежа.

Получатель платежа, проверив правильность подписи оператора платежной системы для квитанции получателя платежа, считает платеж проведенным, и доставляет плательщику данные, подтверждающие проведение платежа.

Совокупность признаков первого варианта способа обеспечивает достижение ранее изложенного технического результата изобретения, заключающегося в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности. Указанный технический результат при осуществлении способа проведения платежей по первому варианту достигается, в частности, тем, что плательщик защищен от нечестного оператора платежной системы тем, что последний обязан отчитываться о проведенных им расходах по платежному сертификату подписанным платежным поручением плательщика, приватность плательщика защищена процедурой изготовления подписи платежного сертификата вслепую, а приватность получателя платежа может быть защищена тем, что при открытии счета получатель платежа не обязан сообщать никаких сведений, позволяющих определить его личность.

Ниже в примере 3 описан частный случай конкретной реализации выбора денежных ключей. структуры платежных сертификатов и операции создания основы платежного сертификата.

Пример 3

Денежные секретные и соответствующие денежные открытые ключи в рамках схемы цифровой подписи, допускающей изготовление цифровой подписи вслепую, могут быть выбраны следующим образом. Выбирается RSA-модуль N как произведение двух простых чисел P и Q и выбираются взаимно простые открытые экспоненты E1, E2, E3. Способы выбора таких данных хорошо известны (B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley& Sons, New York, 2nd edition, 1996; A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997). Открытым денежным ключом является набор данных (N, E), где открытая экспонента E представлена как произведение открытых экспонент E1, E2, E3 в натуральных степенях M1, M2, M3.

Также заранее выбираются номинальные стоимости S1, S2, S3, связанные с открытыми экспонентами E1, E2, E3, а с открытой экспонентой E связывается номинальная стоимость S = M1xS1 + M2xS2 +M3xS3. Для определенности, в данном примере, M1 = 1 рубль, M2 = 100 рублей, M3 = 1000 рублей.

Оператор платежной системы, в этом примере банк, фиксирует публичную одностороннюю функцию F, принимающую значения в множестве натуральных чисел не превосходящих N. В качестве такой функции можно взять одну из признанных хэш-функций (см. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley&Sons, New York, 2nd edition, 1996; A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997), рассматривая ее образ как двоичное разложение целого числа. Вычислители таких функций, то есть средства для их вычисления, также хорошо известны.

Основой платежного сертификата являются данные (Y, X), где F(Y)=X. При этом X является номером платежного сертификата, а Y идентификатором открытого ключа подписи платежного сертификата. При выборе основы платежного сертификата плательщик выбирает секретный ключ подписи DP и соответствующий ему открытый ключ подписи EP в рамках произвольной схемы цифровой подписи и получает основу платежного сертификата (Y, X), где Y = EP, а X = F(EP). Для определенности в данном примере DP и EP являются RSA-ключами.

Ниже в примере 4 описан частный случай конкретной реализации получения подписи платежного сертификата в ходе операции пополнения платежного устройства.

Пример 4

В этом примере используются обозначения и соглашения, принятые в примере 3. Плательщик, желая получить для основы платежного сертификата (Y, X) подпись, соответствующую номиналу 320 рублей, производит маскировку номера X способом. известным из: D. Chaum, Blind Signature Systems, U.S. Patent 4,759,063, 19 Jul 1988, в соответствии с открытой экспонентой E и степенями M1 = 20, M2 = 3, M3 = 0. удовлетворяющими соотношению 320 = M1xS1 + M2xS2 + M3xS3 и получает замаскированные данные X', которые доставляет в банк вместе с номером своего

RU 2157001 C2

RU 2157001 C2

счета и суммой кредитования 320 рублей в качестве денежного запроса.

Банк выбирает денежный секретный ключ, соответствующий сумме кредитования в 320 рублей, выбирая секретную экспоненту D как произведение секретных экспонент D1, D2, D3, соответствующих открытым экспонентам E1, E2, E3, в степенях M1, M2, M3. После этого банк изготавливает данные для демаскировки SIGN' способом из: D. Chaum, Blind Signature Systems, U.S. Patent 4,759,063, 19 Jul 1988, и производит дебетование указанного плательщиком счета на 321 рубль в предположении, что стоимость услуги по изготовлению подписи равна 1 рублю.

Получив данные для демаскировки SIGN' плательщик изготавливает подпись платежного сертификата SIGN демаскировкой полученных данных SIGN' способом, известным из: D. Chaum, Blind Signature Systems, U.S. Patent 4,759,063, 19 Jul 1988, и получает тем самым годный для проведения платежной операции платежный сертификат номинальной стоимостью 326 рублей.

В примере 5 описан частный случай конкретной реализации операции открытия счета у оператора платежной системы. Этот способ может быть, в частности, использован для открытия у оператора платежной системы счета получателя платежа.

Пример 5

Будущий владелец открываемого счета, например получатель платежа, открывает в банке счет, допускающий безопасное удаленное управление. Для этого будущий владелец счета выбирает секретный ключ и открытый ключи подписи счета подписи счета DS и ES, в рамках произвольной схемы цифровой подписи, и доставляет ключ ES по открытой сети в банк. Банк присваивает открываемому счету номер N и создает в хранилище счетов запись, содержащую данные ES, N и иные атрибуты счета. Подписанные банком данные счета доставляются по открытой сети владельцу открываемого счета, который, проверив подпись банка и сохранив ее для разрешения возможных конфликтных ситуаций, считает счет открытым.

В примере 6 описан частный случай конкретной реализации проведения плательщиком платежной операции.

Пример 6

В этом примере используются обозначения и соглашения, принятые в примерах 4, 5.

Плательщик, желая заплатить получателю платежа, который в данном примере является продавцом, 320 рублей за некоторый товар готовит платежные данные PaymentData = (PayerOrder, A), где PayerOrder платежное поручение плательщика, подписанное секретным ключом подписи платежного сертификата DP, а данные A предназначены для продавца и состоят в данном примере из наименования оплачиваемого товара и идентификационных данных лица, которому следует выдать данный товар. Платежное поручение плательщика PayerOrder состоит из открытого ключа подписи платежного сертификата EP, подписи платежного сертификата SIGN, номера счета получателя платежа N и данных C, определяющих условия платежа. В данном примере в качестве C плательщик берет номер счета продавца N и образ заранее оговоренной хэш-функции H от текста обязательства, которое принимает на себя продавец в случае проведения платежа, а именно обязательства предоставить соответствующий товар лицу с указанными идентификационными данными.

Получатель платежа, желая принять платеж, формирует свое платежное поручение SellerOrder = (N, C, PaymentData), подписанное секретным ключом DS, и доставляет его в банк.

Ниже приведен пример конкретной реализации способа проведения платежей по первому варианту.

Пример 7

В этом примере используются обозначения и соглашения, принятые в примере 6.

Банк выбирает денежные ключи, а плательщик выбирает основу платежного сертификата как в примере 3. Операцию пополнения платежного устройства плательщика производят как в примере 4, продавец открывает в банке счет как в примере 5, а плательщик и продавец проводят платежную операцию как в примере 6.

Банк, убедившись, что в списке использованных платежных сертификатов отсутствует запись о платежном сертификате с открытым ключом подписи EP, проверив подпись платежного поручения плательщика PayerOrder открытым ключом подписи EP, проверив подпись платежного поручения продавца SellerOrder открытым ключом подписи счета N, проверив совпадение условий платежа, содержащихся в платежных поручениях плательщика и продавца, и, проверив правильность подписи платежного сертификата SIGN, заносит в список использованных платежных сертификатов запись, включающую открытый ключ EP и подписанное платежное поручение плательщика PayerOrder, кредитует счет получателя платежа и, тем самым, получателя платежа, зачисляя на этот счет сумму 319 рублей, в предположении, что стоимость проведения платежной операции банком равна 1 рублю, сохраняет подписанное поручение получателя платежа SellerOrder в своем информационном хранилище. После этого банк формирует квитанцию продавца, подтверждающую факт кредитования счета с номером N на сумму 319 рублей, подписывает ее и доставляет продавцу, который, проверив правильность подписи банка для полученной квитанции, считает платеж проведенным и сообщает плательщику об успешном проведении платежа.

В качестве других частных случаев способа по первому варианту имеется в виду возможность реализации в виде многих иных комбинаций зависимых пунктов 2-14, а также возможность шифрования, дешифрования и перекодировки данных при их передаче по коммуникационным сетям, которые не меняют сущности данного изобретения. Кроме того, оператор платежной системы при авторизации платежного сертификата может проверять подпись платежного сертификата как открытыми, так и секретными денежными ключами. Помимо этого, при ошибках работы

RU 2157001 C2

RU 2157001 C2

коммуникационных сетей при проведении вовлеченных в проведение платежа операций такие операции могут быть повторены до их успешного завершения без ущерба для вовлеченных сторон.

Указанный выше технический результат при реализации изобретения достигается тем, что способ проведения платежей по второму варианту, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, создании плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одну основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего изготавливают подпись платежного сертификата введением доставленных данных для демаскировки в демаскирующее устройство и осуществляют проверку правильности изготовленной подписи платежного сертификата введением ее и денежного открытого ключа, соответствующего использованному оператором платежной системы денежному секретному ключу, в устройство для проверки подписи, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, отличается тем, что в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи платежного сертификата посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который, при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежным сертификатом, и в случае отсутствия такого счета открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня денежного секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер

RU 2157001 C2

RU 2157001 C2

оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

Указанный выше технический результат в частных случаях конкретной реализации может достигаться, кроме того, тем, что при создании основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификата и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией. В частности, при включении в основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата в качестве этого идентификатора может быть использован сам открытый ключ подписи платежного сертификата. Помимо этого, при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата может быть включен в основу в качестве дополнительного номера.

Кроме того, перед включением в платежные данные платежное поручение плательщика может быть зашифровано одним из открытых ключей для шифрования оператора платежной системы. В этом случае оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования. Более того, оператор платежной системы может осуществлять шифрование своего ответа на платежное поручение получателя платежа.

Кроме того, в условия платежа, содержащиеся в платежном поручении плательщика, могут быть включены данные обязательства получателя платежа перед плательщиком. Более того, при подготовке плательщиком платежных данных данные обязательства получателя платежа перед плательщиком могут быть обработаны наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включены в подготавливаемое платежное поручение плательщика, причем получатель платежа также производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа. В частности, наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

Помимо этого, получатель платежа может подписать данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей подписи и до платежной операции проверить подпись получателя платежа для данных обязательства получателя платежа перед плательщиком.

В частности, при проведении операции пополнения платежного устройства в качестве источника кредитования может быть использован счет плательщика, который предварительно кредитуют при платежной операции. Помимо этого, при проведении операции пополнения платежного устройства в качестве источника кредитования может быть использована банковская карточка.

Помимо этого, при открытии платежного счета, связанного с авторизуемым платежным сертификатом, может быть произведено его предварительное дебетование.

В частности, при проведении платежной операции в качестве плательщика может выступать получатель платежа, а оператор платежной системы может иметь несколько платежных серверов.

Сущность способа проведения платежей по второму варианту состоит в том же, что и по первому варианту, за исключением того, что используют платежные сертификаты, допускающие постепенное расходование своей стоимости. Это выражается в том, что оператор платежной системы при проведении операции авторизации в случае отсутствия в его информационном хранилище сведений об авторизуемом платежном сертификате открывает связанный с данным платежным сертификатом платежный счет и связывает

RU 2157001 C2

RU 2157001 C2

его с открытым ключом подписи платежного сертификата. В случае же наличия в информационном хранилище оператора платежной системы сведений об авторизуемом платежном сертификате, то есть записи о соответствующем платежном счете, оператор платежной системы не отвергает платеж, а проводит его в зависимости от того, покрывает ли сальдо платежного счета, то есть превышение кредита платежного счета над его дебетом, проплачиваемую сумму. Платежный счет, связанный с платежным сертификатом, кредитуется при операциях авторизации оператором платежной системы присланных плательщиком подписей платежных сертификатов в том случае, если уровень доставленной подписи платежного сертификата превышает уровень ранее авторизованной подписи данного платежного сертификата. При этом плательщик может кредитовать свой платежный счет в ходе нескольких операций авторизации, шаг за шагом повышая известный оператору платежной системы уровень платежного сертификата. Это позволяет плательщику ослабить возможность связывания платежного сертификата с источником его кредитования по номинальной стоимости платежного сертификата. Кроме того, плательщик может использовать один и тот же платежный сертификат при нескольких платежных операциях, при некоторых из них доставляя оператору платежной системы данные для кредитования платежного счета, то есть подпись платежного сертификата более высокого уровня, чем уже известна оператору платежной системы. Такие подписи плательщик может изготовить из данных для демаскировки, полученных им при изготовлении вслепую денежной подписи. Помимо этого, сумма платежа может быть произвольной в рамках платежеспособности используемого платежного сертификата, так как ее величина не связана с номинальными стоимостями, соответствующими денежным ключам.

Под платежным счетом имеется в виду счет, допускающий проведение с него платежей путем перевода части суммы счета на другой счет или перевода части суммы счета в иную форму для выдачи их получателю платежа.

Под уровнем платежного сертификата, а также соответствующим ему уровнем подписи и уровнем денежного ключа имеются в виду данные, определяющие денежный ключ в частично упорядоченном множестве денежных ключей таким образом, что при сложении уровней складываются и номинальные стоимости, соответствующие этим денежным уровням.

Ниже приведен пример уровней платежных сертификатов, их подписей и соответствующих им денежных ключей.

Пример 8

В этом примере используются обозначения и соглашения, принятые в примере 3.

Уровнем денежного ключа в данном примере является набор из трех чисел (M1, M2, M3), а частичное упорядочение уровней задано покоординатным упорядочением таких наборов, то есть уровень (M1, M2, M3) больше некоторого другого уровня (K1, K2, K3), если M1 больше K1, M2 больше K2 и M3 больше K3.

Например, уровень подписи SIGN из примера 4 равен (M1, M2, M3) = (20, 3, 0).

Совокупность признаков второго варианта способа обеспечивает достижение ранее изложенного технического результата изобретения, заключающегося в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности. Помимо этого доступны платежи в диапазоне от микроплатежей до платежей бизнес-уровня, время проведения платежа зависит только от быстроты действия сетевых соединений, но не от суммы платежа, число клиентов, которые могут быть обслужены оператором платежной системы, растет пропорционально его ресурсам.

Указанный технический результат при осуществлении способа проведения платежей по второму варианту достигается, в частности, тем, что плательщик защищен от нечестного оператора платежной системы тем, что последний обязан отчитываться о проведенных им расходах по платежному сертификату подписанным платежным поручением плательщика, приватность плательщика защищена процедурой изготовления подписи платежного сертификата вслепую, а приватность получателя платежа может быть защищена тем, что при открытии счета получатель платежа не обязан сообщать никаких сведений, позволяющих определить его личность. Диапазон платежей и независимость времени проведения платежей обеспечены независимостью суммы платежа от номинальных стоимостей, соответствующих денежным ключам. Рост числа клиентов пропорционально ресурсам оператора платежной системы обеспечен тем, что с помощью одного платежного сертификата можно проводить большое число платежей, а число используемых платежных сертификатов может быть ограничено стоимостью операции открытия платежного счета и операции изготовления вслепую денежной подписи.

Ниже приведен пример конкретной реализации способа проведения платежей по второму варианту.

Пример 9

В этом примере используются обозначения и соглашения, принятые в примерах 3, 4, 5. Банк выбирает денежные ключи, а плательщик выбирает основу платежного сертификата, как в примере 3. Операцию пополнения платежного устройства плательщика производят, как в примере 4, а получатель платежа открывает в банке счет, как в примере 5.

Плательщик проводит платежную операцию следующим образом. Желая заплатить продавцу 115.5 рублей за некоторый товар, плательщик готовит платежные данные PaymentData = (PayerOrder, A), где PayerOrder - платежное поручение плательщика, подписанное секретным ключом подписи платежного сертификата DP, а данные A предназначены для продавца и состоят в данном примере из

RU 2157001 C2

RU 2157001 C2

наименования оплачиваемого товара и идентификационных данных лица, которому следует выдать данный товар. Платежное поручение плательщика PayerOrder состоит из открытого ключа подписи платежного сертификата EP, подписи платежного сертификата уменьшенного уровня sign, номера счета получателя платежа N и данных C, определяющих условия платежа C, как и в примере 6. Подпись платежного сертификата уменьшенного уровня sign плательщик изготавливает понижением уровня (M1, M2, M3) = (20, 3, 0) подписи SIGN. В качестве уровня подписи sign плательщик выбирает (K1, K2, K3) = (17, 1, 0), так как соответствующий этой сумме номинал равен 117 рублей, что достаточно для проведения платежа на сумму 115.5 рублей. Подпись sign плательщик в данном примере изготавливает посредством возведения подписи SIGN в степень L, равную произведению открытых экспонент E1, E2, E3 в степенях (M1-K1, M2-K2, M3-K3), что может быть выполнено посредством модулярного экспоненциатора. Получатель платежа в данном примере действует также как и в примере 7.

Банк, убедившись, что в хранилище платежных счетов запись о платежном счете с открытым ключом подписи EP, и, проверив правильность подписи платежного сертификата sign, открывает платежный счет, связанный с открытым ключом EP, кредитует его на сумму 116 рублей, в предположении, что стоимость операции открытия платежного счета 1 рубль, и проверив подпись платежного поручения плательщика PayerOrder открытым ключом подписи EP, проверив подпись платежного поручения продавца SellerOrder открытым ключом подписи счета N, проверив совпадение условий платежа, содержащихся в платежных поручениях плательщика и продавца, заносит в информационное хранилище подписанное платежное поручение плательщика PayerOrder, производит дебетование платежного счета на сумму 115.5 рублей, кредитует на счет получателя платежа на сумму 114.5 рублей, в предположении, что стоимость проведения платежной операции банком равна 1 рублю, сохраняет подписанное поручение получателя платежа SellerOrder в своем информационном хранилище. После этого банк формирует квитанцию продавца, подтверждающую факт кредитования счета с номером N на сумму 114.5 рублей, подписывает ее и доставляет продавцу, который, проверив правильность подписи банка для полученной квитанции, считает платеж проведенным, и сообщает плательщику об успешном проведении платежа.

Оставшаяся на платежном сертификате сумма, равная разности 320 рублей и 117 рублей, может быть доставлена в банк и потрачена при других платежных операциях.

В качестве других частных случаев способа по второму варианту имеется в виду возможность реализации в виде многих иных комбинаций зависимых пунктов 16-29, а также возможность шифрования, дешифрования и перекодировки данных при их передаче по коммуникационным сетям, которые не меняют сущности данного изобретения. Кроме того, оператор платежной системы при авторизации платежного сертификата может проверять подпись платежного сертификата как открытыми, так и секретными денежными ключами. Помимо этого, при ошибках работы коммуникационных сетей при проведении вовлеченных в проведение платежа операций такие операции могут быть повторены до их успешного завершения без ущерба для вовлеченных сторон. В частности, данные, по которым плательщик судит о проведении платежа, могут включать данные, подтверждающие факт проведения платежа и подписанные одним из секретных ключей подписи оператора платежной системы.

Указанный выше технический результат при реализации изобретения достигается тем, что способ проведения платежей по третьему варианту, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, создании плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одну основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего осуществляют проверку правильности доставленных данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, и принимают их в качестве данных для получения подписи платежного сертификата, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операций, при которой подпись и основу используемого

RU 2157001 C2

RU 2157001 C2

при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, отличается тем, что в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи платежного сертификата посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежном сертификатом, и в случае отсутствия такого счета открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня денежного секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством операции пополнения платежного сертификата, при которой выбирают платежный сертификат и формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, в качестве которых берут замаскированную подпись платежного сертификата наибольшего уровня, предварительно изготовленную посредством демаскировки данных для получения подписи платежного сертификата, и доставляют его в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования по денежному запросу, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством обработки содержащихся в запросе данных для изготовления вслепую денежной подписи соответствующим сумме кредитования денежным секретным ключом и доставляет их отправителю денежного запроса, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, и принимает их в качестве данных для получения подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика и подпись для этого платежного поручения, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа

RU 2157001 C2

RU 2157001 C2

посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

Указанный выше технический результат в частных случаях конкретной реализации может достигаться, кроме того, тем, что при создании основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификата и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией. В частности, при включении в основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора может быть использован сам открытый ключ подписи платежного сертификата. Помимо этого, при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата может быть включен в основу в качестве дополнительного номера.

Кроме того, перед включением в платежные данные платежное поручение плательщика может быть зашифровано одним из открытых ключей для шифрования оператора платежной системы. В этом случае оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования. Помимо этого, оператор платежной системы может осуществить шифрование своего ответа на платежное поручение получателя платежа.

Кроме того, в условия платежа, содержащиеся в платежном поручении плательщика, могут быть включены данные обязательства получателя платежа перед плательщиком. Более того, при подготовке плательщиком платежных данных данные обязательства получателя платежа перед плательщиком могут быть обработаны наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включены в подготавливаемое платежное поручение плательщика, причем получатель платежа также производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа. В частности, наперед заданная маскирующая функция может быть выбрана произвольно из множества односторонних функций.

Помимо этого, получатель платежа может подписать данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей подписи и до платежной операции проверить подпись получателя платежа для данных обязательства получателя платежа перед плательщиком.

В частности, при проведении операции пополнения платежного устройства в качестве источника кредитования может быть использован счет плательщика, который предварительно кредитуют при платежной операции. Помимо этого, при проведении операции пополнения платежного устройства в качестве источника кредитования может быть использована банковская карточка.

Помимо этого, при открытии платежного счета, связанного с авторизуемым платежным сертификатом, может быть произведено его предварительное дебетование.

Кроме того, при операции пополнения платежного сертификата формирование денежного запроса может быть произведено в соответствии с единой для всех денежных запросов структурой.

В частности, подпись авторизуемого платежного сертификата может быть изготовлена посредством понижения уровня имеющейся у плательщика подписи платежного сертификата, при проведении платежной операции в качестве плательщика может выступать получатель платежа, а оператор платежной системы может иметь несколько платежных серверов.

Сущность способа проведения платежей по третьему варианту состоит в том же, что и по второму варианту, за исключением того, что плательщику дополнительно доступна операция пополнения своего платежного устройства за счет пополнения уже имеющихся у него платежных сертификатов путем увеличения уровня их подписи с помощью оператора платежной системы, изготавливающего вслепую подпись платежного сертификата повышенного уровня. При этом оператор платежной системы не имеет возможности определить, служит ли изготавливаемые им в ходе изготовления вслепую денежной подписи данные для демаскировки для пополнения уже имеющегося платежного сертификата, или они служат для наполнения вновь созданного платежного сертификата. При этом при пополнении одного и того же платежного сертификата плательщик может использовать различные источники кредитования, не связывая их между собой.

Совокупность признаков третьего варианта способа обеспечивает достижение ранее изложенного технического результата изобретения, заключающегося в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности. Помимо этого доступны платежи в диапазоне от микроплатежей до платежей бизнес-уровня, время проведения платежа зависит только от быстроты действия сетевых соединений, но не от суммы платежа, число

RU 2157001 C2

RU 2157001 C2

клиентов, которые могут быть обслужены оператором платежной системы, растет пропорционально его ресурсам.

Указанный технический результат при осуществлении способа проведения платежей по третьему варианту достигается, в частности, тем, что плательщик защищен от нечестного оператора платежной системы тем, что последний обязан отчитываться о проведенных им расходах по платежному сертификату подписанным платежным поручением плательщика, приватность плательщика защищена процедурой изготовления подписи платежного сертификата вслепую, а приватность получателя платежа может быть защищена тем, что при открытии счета получатель платежа не обязан сообщать никаких сведений, позволяющих определить его личность. Диапазон платежей и независимость времени проведения платежей обеспечены независимостью суммы платежа от номинальных стоимостей, соответствующих денежным ключам. Рост числа клиентов пропорционально ресурсам оператора платежной системы обеспечен тем, что с помощью одного платежного сертификата можно проводить большое число платежей, а число используемых платежных сертификатов может быть ограничено стоимостью операции открытия платежного счета и операции изготовления вслепую денежной подписи.

Ниже приведен пример конкретной реализации способа проведения платежей по третьему варианту.

Пример 10

В этом примере используются обозначения и соглашения, принятые в примере 9. Банк, плательщик и продавец действуют также как и в примере 9, за исключением того, что плательщик в некоторый момент времени после получения им подписи SIGN платежного сертификата уровня (M1, M2, M3) = (20, 3, 0), что соответствует сумме 320 рублей, принимает решение пополнить этот платежный сертификат на 190 рублей. Для этого плательщик формирует денежный запрос в банк точно также как и в примере 4, за исключением того, что вместо маскировки номера X он маскирует имеющуюся у него подпись платежного сертификата SIGN в соответствии с открытой экспонентой, определенной уровнем (U1, U2, U3), где U1= 90, U2=1, U3=0 удовлетворяют соотношению 190 = U1xS1 + U2xS2 +U3xS3 и получает замаскированные данные X', которые доставляет в банк вместе с указанием, возможно иного, источника кредитования и суммой кредитования 190 рублей в качестве денежного запроса.

Далее, банк действует как и в примере 4, выбирает денежный секретный ключ, соответствующий сумме кредитования в 190 рублей, изготавливает данные для демаскировки SIGN'. Получив данные для демаскировки SIGN', плательщик изготавливает новую подпись платежного сертификата SIGN уровня (M1 + U1, M2 + U2, M3 + U3) = (110, 4, 0) демаскировкой полученных данных SIGN' и получает тем самым годный для проведения платежной операции платежный сертификат номинальной стоимостью 510 рублей.

В качестве других частных случаев способа по третьему варианту имеется в виду возможность реализации в виде многих иных комбинаций зависимых пунктов 31-46, а также возможность шифрования, дешифрования и перекодировки данных при их передаче по коммуникационным сетям, которые не меняют сущности данного изобретения. Кроме того, оператор платежной системы при авторизации платежного сертификата может проверять подпись платежного сертификата как открытыми, так и секретными денежными ключами. Помимо этого, при ошибках работы коммуникационных сетей при проведении вовлеченных в проведение платежа операций такие операции могут быть повторены до их успешного завершения без ущерба для вовлеченных сторон.

Указанный выше технический результат при реализации изобретения достигается тем, что способ проведения платежей по четвертому варианту, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, создании плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одну основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего изготавливают подпись платежного сертификата введением доставленных данных для демаскировки в демаскирующее устройство и осуществляют проверку правильности изготовленной подписи платежного сертификата введением ее и денежного открытого ключа, соответствующего использованному оператором платежной системы денежному секретному ключу, в устройство для проверки подписи, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного

RU 2157001 C2

RU 2157001 C2

сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, отличается тем, что в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи платежного сертификата посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежном сертификатом, и в случае отсутствия такого счета открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию перевода с одного из платежных сертификатов на другой, один из которых выбирают в качестве исходного платежного сертификата, а другой в качестве целевого платежного сертификата, формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, в качестве которых берут предварительно изготовленную замаскированную подпись целевого платежного сертификата наибольшего уровня, и платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи исходного платежного сертификата, причем в платежное поручение плательщика включают идентификатор исходного платежного сертификата и сумму перевода, денежный запрос доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который проверяет правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи исходного платежного сертификата, осуществляют кредитование целевого платежного сертификата, при котором производят дебетование платежного счета, связанного с исходным платежным сертификатом, создают при изготовлении вслепую денежной подписи данные для демаскировки посредством обработки содержащихся в денежном запросе данных для изготовления вслепую денежной подписи денежным секретным ключом, соответствующим сумме кредитования целевого платежного сертификата, и доставляют их плательщику, который осуществляет проверку правильности доставленных ему данных дли демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, и принимает их в качестве данных для получения подписи целевого платежного сертификата, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня денежного секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя

RU 2157001 C2

RU 2157001 C2

платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

Указанный выше технический результат в частных случаях конкретной реализации может достигаться, кроме того, тем, что при создании основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификата и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией. В частности, при включении в основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата в качестве этого идентификатора может быть использован сам открытый ключ подписи платежного сертификата. Помимо этого, при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата может быть включен в основу в качестве дополнительного номера.

Кроме того, перед включением в платежные данные платежное поручение плательщика может быть зашифровано одним из открытых ключей для шифрования оператора платежной системы. В этом случае оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования. Более того, оператор платежной системы может осуществлять шифрование своего ответа на платежное поручение получателя платежа.

В частности, в условия платежа, содержащиеся в платежном поручении плательщика, могут быть включены данные обязательства получателя платежа перед плательщиком. Кроме того, при подготовке плательщиком платежных данных данные обязательства получателя платежа перед плательщиком могут быть обработаны наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включены в подготавливаемое платежное поручение плательщика, причем получатель платежа также производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа. В частности, наперед заданная маскирующая функция может быть выбрана произвольно из множества односторонних функций. Помимо этого, получатель платежа может подписать данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей подписи и до платежной операции проверить подпись получателя платежа для данных обязательства получателя платежа перед плательщиком.

Кроме того, при проведении операции пополнения платежного устройства в качестве источника кредитования может быть использован счет плательщика, который предварительно кредитуют при платежной операции. Помимо этого, при проведении операции пополнения платежного устройства в качестве источника кредитования может быть использована банковская карточка.

В частности, при открытии платежного счета, связанного с авторизуемым платежным сертификатом, может быть произведено его предварительное дебетование. Помимо этого, при операции пополнения платежного сертификата формирование денежного запроса может производиться в соответствии с единой для всех денежных запросов структурой. Кроме того, подпись авторизуемого платежного сертификата может быть изготовлена посредством понижения уровня имеющейся у плательщика подписи платежного сертификата.

Более того, при проведении платежной операции в качестве плательщика может выступать получатель платежа, а оператор платежной системы может иметь несколько платежных серверов.

Сущность способа проведения платежей по четвертому варианту состоит в том же, что и по третьему варианту, за исключением того, что плательщику дополнительно доступна операция перевода с одного своего платежного сертификата на другой. При этом данный перевод производится посредством изготовления вслепую подписи целевого платежного сертификата, то есть того платежного сертификата, номинальная стоимость которого увеличивается при этой операции. Кредитование целевого платежного сертификата происходит за счет платежного

RU 2157001 C2

RU 2157001 C2

счета, связанного с исходным платежным сертификатом.

Совокупность признаков четвертого варианта способа обеспечивает достижение ранее изложенного технического результата изобретения, заключающегося в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей, приватности. Помимо этого доступны платежи в диапазоне от микроплатежей до платежей бизнес-уровня, время проведения платежа зависит только от быстроты действия сетевых соединений, но не от суммы платежа, число клиентов, которые могут быть обслужены оператором платежной системы, растет пропорционально его ресурсам.

Указанный технический результат при осуществлении способа проведения платежей по четвертому варианту достигается, в частности, тем, что плательщик защищен от нечестного оператора платежной системы тем, что последний обязан отчитываться о проведенных им расходах по платежному сертификату подписанным платежным поручением плательщика, приватность плательщика защищена процедурой изготовления подписи платежного сертификата вслепую, а приватность получателя платежа может быть защищена тем, что при открытии счета получатель платежа не обязан сообщать никаких сведений, позволяющих определить его личность. Диапазон платежей и независимость времени проведения платежей обеспечены независимостью суммы платежа от номинальных стоимостей, соответствующих денежным ключам. Рост числа клиентов пропорционально ресурсам оператора платежной системы обеспечен тем, что с помощью одного платежного сертификата можно проводить большое число платежей, а число используемых платежных сертификатов может быть ограничено стоимостью операции открытия платежного счета и операции изготовления вслепую денежной подписи.

Ниже приведен пример конкретной реализации способа проведения платежей по четвертому варианту.

Пример 11

В этом примере используются обозначения и соглашения, принятые в примере 10. Банк, плательщик и продавец действуют также как и в примере 10, за исключением того, что плательщик как в примере 4 или как в примере 10 получает платежный сертификат, который принимает за целевой. После этого плательщик пополняет целевой платежный сертификат как и в примере 10, за исключением того, что в качестве источника кредитования указывает платежный счет, связанный с исходным платежным сертификатом. При этом платежное поручение банку подписывается секретным ключом подписи исходного платежного сертификата, а банк сохраняет это подписанное поручение в информационном хранилище для предъявления в случае возникновения конфликтной ситуации.

В качестве других частных случаев способа по четвертому варианту имеется в виду возможность реализации в виде многих иных комбинаций зависимых пунктов 48-63, а также возможность шифрования, дешифрования и перекодировки данных при их передаче по коммуникационным сетям, которые не меняют сущности данного изобретения. Кроме того, оператор платежной системы при авторизации платежного сертификата может проверять подпись платежного сертификата как открытыми, так и секретными денежными ключами. Помимо этого, при ошибках работы коммуникационных сетей при проведении вовлеченных в проведение платежа операций такие операции могут быть повторены до их успешного завершения без ущерба для вовлеченных сторон. Помимо этого при переводе с одного платежного сертификата на другой можно использовать предложенный в D. Chaum, Returned Value Blind Signature Systems, U.S. Patent 4,949,380, 14 Aug 1990 способ получения "слепой сдачи" для получения остатка исходного платежного сертификата, размер которого будет скрыт от оператора платежной системы.

Указанный выше технический результат при реализации изобретения достигается тем, что способ проведения платежей по пятому варианту, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одну основу платежного сертификата, которая включает его номер, и получает подпись платежного сертификата посредством изготовления вслепую денежной подписи оператором платежной системы, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, причем при проверке платежеспособности используемого при платеже платежного сертификата оператор платежной системы проводит операцию его авторизации, при которой по наличию информации об авторизуемом платежном сертификате в информационном хранилище отказывают в авторизации, а по ее отсутствию осуществляют проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, и в случае правильности заносят информацию об авторизуемом платежном сертификате в информационное хранилище, после чего формируют ответ оператора платежной системы на платежное поручение получателя платежа и доставляют

RU 2157001 C2

RU 2157001 C2

его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, отличается тем, что в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи платежного сертификата посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении операции пополнения платежного устройства плательщик дополнительно формирует платежное требование, включающее замаскированную подпись выбранного платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и подписанное одним из секретных ключей подписи плательщика, и доставляет его промежуточному плательщику, который проверяет подпись для платежного требования открытым ключом подписи плательщика, соответствующим использованному секретному ключу подписи плательщика, формирует и доставляет в платежный сервер оператора платежной системы денежный запрос, который включает дополнительно замаскированную промежуточным плательщиком полученную от плательщика замаскированную подпись выбранного платежного сертификата и идентификатор счета промежуточного плательщика, причем денежный запрос подписывают секретным ключом счета промежуточного плательщика, а оператор платежной системы проверяет подпись денежного запроса промежуточного плательщика открытым ключом счета, идентификатор которого содержится в денежном запросе, осуществляет дебетование этого счета, создает при изготовлении вслепую денежной подписи данные для демаскировки, которые доставляют промежуточному плательщику, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, производит их демаскировку, результат которой доставляют плательщику, который изготавливает подпись платежного сертификата демаскировкой полученных от промежуточного плательщика данных для демаскировки, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, в информационное хранилище при авторизации платежного сертификата заносят подписанное платежное поручение плательщика, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

Указанный выше технический результат в частных случаях конкретной реализации может достигаться, кроме того, тем, что при создании основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификата и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством

RU 2157001 C2

RU 2157001 C2

выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией. В частности, при включении в основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата в качестве этого идентификатора может быть использован сам открытый ключ подписи платежного сертификата. Помимо этого, при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата может быть включен в основу в качестве дополнительного номера.

Кроме того, перед включением в платежные данные платежное поручение плательщика может быть зашифровано одним из открытых ключей для шифрования оператора платежной системы. В этом случае оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования. Более того, оператор платежной системы может осуществить шифрование своего ответа на платежное поручение получателя платежа.

В частности, в условия платежа, содержащиеся в платежном поручении плательщика, могут быть включены данные обязательства получателя платежа перед плательщиком. Более того, при подготовке плательщиком платежных данных данные обязательства получателя платежа перед плательщиком могут быть обработаны наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включены в подготавливаемое платежное поручение плательщика, причем получатель платежа также производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа. В частности, наперед заданная маскирующая функция может быть выбрана произвольно из множества односторонних функций. Помимо этого, получатель платежа может подписать данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей подписи и до платежной операции проверить подпись получателя платежа для данных обязательства получателя платежа перед плательщиком.

Кроме того, при проведении операции пополнения платежного устройства в качестве источника кредитования может быть использован счет плательщика, который предварительно кредитуют при платежной операции. Помимо этого, при проведении операции пополнения платежного устройства в качестве источника кредитования может быть использована банковская карточка.

Кроме того, при проведении платежной операции в качестве плательщика может выступать получатель платежа, а оператор платежной системы может иметь несколько платежных серверов.

Сущность способа проведения платежей по пятому варианту состоит в том же, что и по первому варианту, за исключением того, что плательщик получает подпись платежного сертификата посредством промежуточного плательщика, который производит платеж со своего счета на платежный сертификат плательщика. При этом промежуточный плательщик применяет дополнительную маскировку и, соответственно, демаскировку проходящих через него данных для денежной подписи.

Совокупность признаков пятого варианта способа обеспечивает достижение ранее изложенного технического результата изобретения, заключающегося в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности.

Указанный технический результат при осуществлении способа проведения платежей по пятому варианту достигается, в частности, тем, что плательщик защищен от нечестного оператора платежной системы тем, что последний обязан отчитываться о проведенных им расходах по платежному сертификату подписанным платежным поручением плательщика, приватность плательщика защищена процедурой изготовления подписи платежного сертификата вслепую, а приватность получателя платежа может быть защищена тем, что при открытии счета получатель платежа не обязан сообщать никаких сведений, позволяющих определить его личность.

Ниже приведен пример конкретной реализации способа проведения платежей по пятому варианту.

Пример 12

В этом примере используются обозначения и соглашения, принятые в примере 7. Банк, плательщик и продавец действуют также как и в примере 7, за исключением того, что плательщик доставляет замаскированные данные X' промежуточному плательщику, который производит их дополнительную маскировку и, соответственно, демаскировку полученных от банка данных для демаскировки точно так, как плательщик производит маскировку и демаскировку в примере 4.

В качестве других частных случаев способа по пятому варианту имеется в виду возможность реализации в виде многих иных комбинаций зависимых пунктов 65-77, а также возможность шифрования, дешифрования и перекодировки данных при их передаче по коммуникационным сетям, которые не меняют сущности данного изобретения. Кроме того, оператор платежной системы при авторизации платежного сертификата может проверять подпись платежного сертификата как открытыми, так и секретными денежными ключами. Помимо этого, при ошибках работы коммуникационных сетей при проведении вовлеченных в проведение платежа операций такие операции могут быть повторены до их успешного завершения без ущерба для вовлеченных сторон.

Указанный выше технический результат при реализации изобретения достигается тем, что способ проведения платежей по шестому

RU 2157001 C2

RU 2157001 C2

варианту, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, создании плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик получает подпись платежного сертификата посредством изготовления вслепую денежной подписи оператором платежной системы, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, отличается тем, что в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи платежного сертификата посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежном сертификатом, и в случае отсутствия такого счета открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня денежного секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством перевода со счета промежуточного плательщика, при которой плательщик дополнительно формирует платежное требование, включающее замаскированную подпись выбранного платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и подписанное одним из секретных ключей подписи плательщика, и доставляет его промежуточному плательщику, который проверяет подпись для платежного требования открытым ключом подписи плательщика, соответствующим использованному плательщиком секретному ключу подписи, формирует и доставляет в платежный сервер оператора платежной системы денежный запрос, который включает дополнительно замаскированную промежуточным плательщиком полученную от плательщика замаскированную подпись выбранного платежного сертификата и идентификатор счета промежуточного плательщика, причем денежный запрос подписывают секретным ключом счета промежуточного плательщика, а оператор платежной системы проверяет подпись денежного запроса промежуточного плательщика открытым ключом счета, идентификатор которого содержится в денежном запросе, осуществляет дебетование этого счета, создает при изготовлении вслепую денежной подписи данные для демаскировки, которые доставляют промежуточному плательщику, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, производит их демаскировку, результат которой доставляют плательщику, который изготавливает подпись платежного сертификата демаскировкой полученных от промежуточного плательщика данных для демаскировки, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных

RU 2157001 C2

RU 2157001 C2

сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

Указанный выше технический результат в частных случаях конкретной реализации может достигаться, кроме того, тем, что при создании основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификата и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией. В частности, при включении в основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата в качестве этого идентификатора может быть использован сам открытый ключ подписи платежного сертификата. Помимо этого, при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата может быть включен в основу в качестве дополнительного номера.

Кроме того, перед включением в платежные данные платежное поручение плательщика может быть зашифровано одним из открытых ключей для шифрования оператора платежной системы. В этом случае оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования. Более того, оператор платежной системы может осуществлять шифрование своего ответа на платежное поручение получателя платежа.

Кроме того, в условия платежа, содержащиеся в платежном поручении плательщика, могут быть включены данные обязательства получателя платежа перед плательщиком. Более того, при подготовке плательщиком платежных данных данные обязательства получателя платежа перед плательщиком могут быть обработаны наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включены в подготавливаемое платежное поручение плательщика, причем получатель платежа также производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа. В частности, наперед заданная маскирующая функция может быть выбрана произвольно из множества односторонних функций. Помимо этого, получатель платежа может подписать данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей подписи и до платежной операции проверить подпись получателя платежа для данных обязательства получателя платежа перед плательщиком.

В частности, при проведении операции пополнения платежного устройства в качестве источника кредитования может быть использован счет плательщика, который предварительно кредитуют при платежной операции. Помимо этого, при проведении операции пополнения платежного устройства в качестве источника кредитования может быть использована банковская карточка.

Кроме того, при открытии платежного счета, связанного с авторизуемым платежным сертификатом, может быть произведено его предварительное дебетование. Помимо этого, при проведении платежной операции в качестве плательщика может выступать получатель платежа, а оператор платежной системы может иметь несколько платежных серверов.

Сущность способа проведения платежей

RU 2157001 C2

RU 2157001 C2

по шестому варианту состоит в том же, что и по второму варианту, за исключением того, что плательщик получает подпись платежного сертификата посредством промежуточного плательщика, который производит платеж со своего счета на платежный сертификат плательщика. При этом промежуточный плательщик применяет дополнительную маскировку и, соответственно, демаскировку проходящих через него данных для денежной подписи.

Совокупность признаков шестого варианта способа обеспечивает достижение ранее изложенного технического результата изобретения, заключающегося в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности. Помимо этого доступны платежи в диапазоне от микроплатежей до платежей бизнес-уровня, время проведения платежа зависит только от быстроты действия сетевых соединений, но не от суммы платежа, число клиентов, которые могут быть обслужены оператором платежной системы, растет пропорционально его ресурсам.

Указанный технический результат при осуществлении способа проведения платежей по шестому варианту достигается, в частности, тем, что плательщик защищен от нечестного оператора платежной системы тем, что последний обязан отчитываться о проведенных им расходах по платежному сертификату подписанным платежным поручением плательщика, приватность плательщика защищена процедурой изготовления подписи платежного сертификата вслепую, а приватность получателя платежа может быть защищена тем, что при открытии счета получатель платежа не обязан сообщать никаких сведений, позволяющих определить его личность. Диапазон платежей и независимость времени проведения платежей обеспечены независимостью суммы платежа от номинальных стоимостей, соответствующих денежным ключам. Рост числа клиентов пропорционально ресурсам оператора платежной системы обеспечен тем, что с помощью одного платежного сертификата можно проводить большое число платежей, а число используемых платежных сертификатов может быть ограничено стоимостью операции открытия платежного счета и операции изготовления вслепую денежной подписи.

Ниже приведен пример конкретной реализации способа проведения платежей по шестому варианту.

Пример 13

В этом примере используются обозначения и соглашения, принятые в примере 10. Банк, плательщик и продавец действуют также как и в примере 10, за исключением того, что плательщик при пополнении своего платежного устройства доставляет замаскированные как и в примере 4 данные X' промежуточному плательщику, который производит их дополнительную маскировку и, соответственно, демаскировку полученных от банка данных для демаскировки точно так, как плательщик производит маскировку и демаскировку в примере 4.

В качестве других частных случаев способа по шестому варианту имеется в виду возможность реализации в виде многих иных комбинаций зависимых пунктов 79-92, а также возможность шифрования, дешифрования и перекодировки данных при их передаче по коммуникационным сетям, которые не меняют сущности данного изобретения. Кроме того, оператор платежной системы при авторизации платежного сертификата может проверять подпись платежного сертификата как открытыми, так и секретными денежными ключами. Помимо этого, при ошибках работы коммуникационных сетей при проведении вовлеченных в проведение платежа операций такие операции могут быть повторены до их успешного завершения без ущерба для вовлеченных сторон.

Указанный выше технический результат при реализации изобретения достигается тем, что способ проведения платежей по седьмому варианту, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, создании плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик получает подпись платежного сертификата посредством изготовления вслепую денежной подписи оператором платежной системы, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежей системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, отличается тем, что в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи

RU 2157001 C2

RU 2157001 C2

платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи платежного сертификата посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежным сертификатом, и в случае отсутствия такого счета, открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня денежного секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством перевода со счета промежуточного плательщика, при которой плательщик дополнительно формирует платежное требование, включающее замаскированную подпись выбранного платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и подписанное одним из секретных ключей подписи плательщика, и доставляет его промежуточному плательщику, который проверяет подпись для платежного требования открытым ключом подписи плательщика, соответствующим использованному плательщиком секретному ключу подписи, формирует и доставляет в платежный сервер оператора платежной системы денежный запрос, который включает дополнительно замаскированную промежуточным плательщиком полученную от плательщика замаскированную подпись выбранного платежного сертификата и идентификатор счета промежуточного плательщика, причем денежный запрос подписывают секретным ключом счета промежуточного плательщика, а оператор платежной системы проверяет подпись денежного запроса промежуточного плательщика открытым ключом счета, идентификатор которого содержится в денежном запросе, осуществляет дебетование этого счета, создает при изготовлении вслепую денежной подписи данные для демаскировки, которые доставляют промежуточному плательщику, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, производит их демаскировку, результат которой доставляют плательщику, который изготавливает подпись платежного сертификата демаскировкой полученных от промежуточного плательщика данных для демаскировки, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством операции пополнения платежного сертификата, при которой выбирают платежный сертификат и формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, в качестве которых берут замаскированную подпись платежного сертификата наибольшего уровня, предварительно изготовленную посредством демаскировки данных для получения подписи платежного сертификата, и доставляют его в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования по денежному запросу, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством обработки содержащихся в запросе данных для изготовления вслепую денежной подписи соответствующим сумме кредитования денежным секретным ключом и доставляет их отправителю денежного запроса, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, и принимает их в качестве данных для получения подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика и подпись для этого платежного поручения, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из

RU 2157001 C2

RU 2157001 C2

секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

Указанный выше технический результат в частных случаях конкретной реализации может достигаться, кроме того, тем, что при создании основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификата и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией. В частности, при включении в основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора может быть использован сам открытый ключ подписи платежного сертификата. Помимо этого, при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата может быть включен в основу в качестве дополнительного номера.

Кроме того, перед включением в платежные данные платежное поручение плательщика может быть зашифровано одним из открытых ключей для шифрования оператора платежной системы. В этом случае оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования. Более того, оператор платежной системы может осуществлять шифрование своего ответа на платежное поручение получателя платежа.

Кроме того, в условия платежа, содержащиеся в платежном поручении плательщика, могут быть включены данные обязательства получателя платежа перед плательщиком. Более того, при подготовке плательщиком платежных данных данные обязательства получателя платежа перед плательщиком могут быть обработаны наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включены в подготавливаемое платежное поручение плательщика, причем получатель платежа также производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа. В частности, наперед заданная маскирующая функция может быть выбрана произвольно из множества односторонних функций. Помимо этого, получатель платежа может подписать данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей подписи и до платежной операции проверить подпись получателя платежа для данных обязательства получателя платежа перед плательщиком.

Кроме того, при проведении операции пополнения платежного устройства в качестве источника кредитования может быть использован счет плательщика, который предварительно кредитуют при платежной операции. Помимо этого, при проведении операции пополнения платежного устройства в качестве источника кредитования может быть использована банковская карточка.

Кроме того, при открытии платежного счета, связанного с авторизуемым платежным сертификатом, может быть произведено его предварительное дебетование. Помимо этого, при операции пополнения платежного сертификата формирование денежного запроса может быть произведено в соответствии с единой для всех денежных запросов структурой. К тому же подпись авторизуемого платежного сертификата может быть изготовлена посредством понижения уровня имеющейся у плательщика подписи платежного сертификата. Более того, при проведении платежной операции в качестве плательщика может выступать получатель платежа, а оператор платежной системы может иметь несколько платежных серверов.

Сущность способа проведения платежей по седьмому варианту состоит в том же, что и по третьему варианту, за исключением того, что плательщик получает подпись платежного сертификата посредством промежуточного плательщика, который производит платеж со своего счета на платежный сертификат плательщика. При этом промежуточный плательщик применяет дополнительную маскировку и, соответственно, демаскировку

RU 2157001 C2

RU 2157001 C2

проходящих через него данных для денежной подписи.

Совокупность признаков седьмого варианта способа обеспечивает достижение ранее изложенного технического результата изобретения, заключающегося в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности. Помимо этого доступны платежи в диапазоне от микроплатежей до платежей бизнес-уровня, время проведения платежа зависит только от быстроты действия сетевых соединений, но не от суммы платежа, число клиентов, которые могут быть обслужены оператором платежной системы, растет пропорционально его ресурсам.

Указанный технический результат при осуществлении способа проведения платежей по седьмому варианту достигается, в частности, тем, что плательщик защищен от нечестного оператора платежной системы тем, что последний обязан отчитываться о проведенных им расходах по платежному сертификату подписанным платежным поручением плательщика, приватность плательщика защищена процедурой изготовления подписи платежного сертификата вслепую, а приватность получателя платежа может быть защищена тем, что при открытии счета получатель платежа не обязан сообщать никаких сведений, позволяющих определить его личность. Диапазон платежей и независимость времени проведения платежей обеспечены независимостью суммы платежа от номинальных стоимостей, соответствующих денежным ключам. Рост числа клиентов пропорционально ресурсам оператора платежной системы обеспечен тем, что с помощью одного платежного сертификата можно проводить большое число платежей, а число используемых платежных сертификатов может быть ограничено стоимостью операции открытия платежного счета и операции изготовления вслепую денежной подписи.

Ниже приведен пример конкретной реализации способа проведения платежей по седьмому варианту.

Пример 14

В этом примере используются обозначения и соглашения, принятые в примере 10. Банк, плательщик и продавец действуют также как и в примере 10, за исключением того, что плательщик при пополнении своего платежного устройства доставляет замаскированные, как и в примере 4, данные X' промежуточному плательщику, который производит их дополнительную маскировку и, соответственно, демаскировку полученных от банка данных для демаскировки точно так, как плательщик производит маскировку и демаскировку в примере 4.

В качестве других частных случаев способа по седьмому варианту имеется в виду возможность реализации в виде многих иных комбинаций зависимых пунктов 94-109, а также возможность шифрования, дешифрования и перекодировки данных при их передаче по коммуникационным сетям, которые не меняют сущности данного изобретения. Кроме того, оператор платежной системы при авторизации платежного сертификата может проверять подпись платежного сертификата как открытыми, так и секретными денежными ключами. Помимо этого, при ошибках работы коммуникационных сетей при проведении вовлеченных в проведение платежа операций такие операции могут быть повторены до их успешного завершения без ущерба для вовлеченных сторон.

Формула изобретения:

1. Способ проведения платежей, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одну основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего изготавливают подпись платежного сертификата введением доставленных данных для демаскировки в демаскирующее устройство и осуществляют проверку правильности изготовленной подписи платежного сертификата введением ее и денежного открытого ключа, соответствующего использованному оператором платежной системы денежному секретному ключу, в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, причем при проверке платежеспособности используемого при платеже платежного сертификата оператор платежной системы проводит операцию его

RU 2157001 C2

RU 2157001 C2

авторизации, при которой по наличию информации об авторизуемом платежном сертификате в информационном хранилище отказывают в авторизации, а по ее отсутствию осуществляют проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, и в случае правильности заносят информацию об авторизуемом платежном сертификате в информационное хранилище, после чего формируют ответ оператора платежной системы на платежное поручение получателя платежа и доставляют его посредством коммуникационных сетей получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, отличающийся тем, что в основу платежного сертификата дополнительно включает идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного с соответствующим ему секретным ключом подписи платежного сертификата посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа посредством генератора ключей выбирает секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством введения его и секретного ключа подписи счета получателя платежа в подписывающее устройство, а изготовленную подпись доставляют посредством коммутационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, в информационное хранилище при авторизации платежного сертификата заносят подписанное платежное поручение плательщика, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

2. Способ проведения платежей по п.1, отличающийся тем, что при создании основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификата и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

3. Способ проведения платежей по п.1, отличающийся тем, что при включении в основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

4. Способ проведения платежей по любому из п.1 или 2, или 3, отличающийся тем, что при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

5. Способ проведения платежей по п.1, отличающийся тем, что перед включением в платежные данные платежного поручения плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

RU 2157001 C2

RU 2157001 C2

6. Способ проведения платежей по п.1, отличающийся тем, что оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

7. Способ проведения платежей по п.1, отличающийся тем, что в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

8. Способ проведения платежей по п.7, отличающийся тем, что при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

9. Способ проведения платежей по п.8, отличающийся тем, что наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

10. Способ проведения платежей по п.1, отличающийся тем, что получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей подписи, получатель платежа до платежной операции проверяет подпись получателя платежа для данных обязательства получателя платежа перед плательщиком.

11. Способ проведения платежей по п.1, отличающийся тем, что при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

12. Способ проведения платежей по п.1, отличающийся тем, что при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

13. Способ проведения платежей по любому из пп.1 - 12, отличающийся тем, что при проведении платежной операции в качестве плательщика выступает получатель платежа.

14. Способ проведения платежей по любому из пп.1 - 13, отличающийся тем, что имеется по меньшей мере два платежных сервера оператора платежной системы.

15. Способ проведения платежей, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, создании плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одну основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по полученному денежному запросу определяют источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего изготавливают подпись платежного сертификата введением доставленных данных для демаскировки в демаскирующее устройство и осуществляют проверку правильности изготовленной подписи платежного сертификата введением ее и денежного открытого ключа, соответствующего использованному оператором платежной системы денежному секретному ключу, в устройство для проверки подписи, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммутационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, отличающийся тем, что в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи платежного сертификата посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством

RU 2157001 C2

RU 2157001 C2

коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляют поиск платежного счета, связанного с авторизуемым им платежным сертификатом, и в случае отсутствия такого счета, открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня денежного секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

16. Способ проведения платежей по п.15, отличающийся тем, что при создании основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификата и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

17. Способ проведения платежей по п.15, отличающийся тем, что при включении в основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

18. Способ проведения платежей по любому из пп.15, или 16, или 17, отличающийся тем, что при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

19. Способ проведения платежей по п.15, отличающийся тем, что перед включением в платежные данные платежного поручения плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

20. Способ проведения платежей по п.15, отличающийся тем, что оператор платежной системы осуществляет шифрование своего

RU 2157001 C2

RU 2157001 C2

ответа на платежное поручение получателя платежа.

21. Способ проведения платежей по п.15, отличающийся тем, что в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

22. Способ проведения платежей по п.21, отличающийся тем, что при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

23. Способ проведения платежей по п.22, отличающийся тем, что наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

24. Способ проведения платежей по п.15, отличающийся тем, что получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей подписи, получатель платежа до платежной операции проверяет подпись получателя платежа для данных обязательства получателя платежа перед плательщиком.

25. Способ проведения платежей по п.15, отличающийся тем, что при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

26. Способ проведения платежей по п.15, отличающийся тем, что при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

27. Способ проведения платежей по п.15, отличающийся тем, что при открытии платежного счета, связанного с авторизуемым платежным сертификатом, производят его предварительное дебетование.

28. Способ проведения платежей по любому из пп.15 - 27, отличающийся тем, что при проведении платежной операции в качестве плательщика выступает получатель платежа.

29. Способ проведения платежей по любому из пп.15 - 28, отличающийся тем, что имеется по меньшей мере два платежных сервера оператора платежной системы.

30. Способ проведения платежей, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, создании плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одну основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего осуществляют проверку правильности доставленных данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, и принимают их в качестве данных для получения подписи платежного сертификата, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, отличающийся тем, что в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи платежного сертификата посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством

RU 2157001 C2

RU 2157001 C2

коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляют поиск платежного счета, связанного с авторизуемым им платежным сертификатом, и в случае отсутствия такого счета, открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня денежного секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством операции пополнения платежного сертификата, при которой выбирают платежный сертификат и формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, в качестве которых берут замаскированную подпись платежного сертификата наибольшего уровня, предварительно изготовленную посредством демаскировки данных для получения подписи платежного сертификата, и доставляют его в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования по денежному запросу, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством обработки содержащихся в запросе данных для изготовления вслепую денежной подписи соответствующим сумме кредитования денежным секретным ключом и доставляет их отправителю денежного запроса, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, и принимает их в качестве данных для получения подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика и подпись для этого платежного поручения, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляют проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

31. Способ проведения платежей по п.30, отличающийся тем, что при создании основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификата и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел

RU 2157001 C2

RU 2157001 C2

дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

32. Способ проведения платежей по п.30, отличающийся тем, что при включении в основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

33. Способ проведения платежей по любому из пп.30, или 31, или 32, отличающийся тем, что при включении в основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата его включают в основу в качестве дополнительного номера.

34. Способ проведения платежей по п.30, отличающийся тем, что перед включением в платежные данные платежного поручения плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

35. Способ проведения платежей по п.30, отличающийся тем, что оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

36. Способ проведения платежей по п.30, отличающийся тем, что в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

37. Способ проведения платежей по п.36, отличающийся тем, что при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

38. Способ проведения платежей по п.37, отличающийся тем, что наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

39. Способ проведения платежей по п.30, отличающийся тем, что получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей подписи, получатель платежа до платежной операции проверяет подпись получателя платежа для данных обязательства получателя платежа перед плательщиком.

40. Способ проведения платежей по п.30, отличающийся тем, что при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

41. Способ проведения платежей по п.30, отличающийся тем, что при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

42. Способ проведения платежей по п.30, отличающийся тем, что при открытии платежного счета, связанного с авторизуемым платежном сертификатом, производят его предварительное дебетирование.

43. Способ проведения платежей по п.30, отличающийся тем, что при операции пополнения платежного сертификата формирование денежного запроса производят в соответствии с единой для всех денежных запросов структурой.

44. Способ проведения платежей по п.30, отличающийся тем, что подпись авторизуемого платежного сертификата изготавливают посредством понижения уровня имеющейся у плательщика подписи платежного сертификата.

45. Способ проведения платежей по любому из пп.30 - 44, отличающийся тем, что при проведении платежной операции в качестве плательщика выступает получатель платежа.

46. Способ проведения платежей по пп.30 - 45, отличающийся тем, что имеется по меньшей мере два платежных сервера оператора платежной системы.

47. Способ проведения платежей, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, создании плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одну основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего изготавливают подпись платежного сертификата введением доставленных данных для демаскировки в демаскирующее устройство и осуществляют проверку

RU 2157001 C2

RU 2157001 C2

правильности изготовленной подписи платежного сертификата введением ее и денежного открытого ключа, соответствующего использованному оператором платежной системы денежному секретному ключу, в устройство для проверки подписи, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, отличающийся тем, что в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи платежного сертификата посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежным сертификатом, и в случае отсутствия такого счета открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию перевода с одного из платежных сертификатов на другой, один из которых выбирают в качестве исходного платежного сертификата, а другой в качестве целевого платежного сертификата, формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, в качестве которых берут предварительно изготовленную замаскированную подпись целевого платежного сертификата наибольшего уровня, и платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи исходного платежного сертификата, причем в платежное поручение плательщика включают идентификатор исходного платежного сертификата и сумму перевода, денежный запрос доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который проверяет правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи исходного платежного сертификата, осуществляют кредитование целевого платежного сертификата, при котором производят дебетование платежного счета, связанного с исходным платежным сертификатом, создают при изготовлении вслепую денежной подписи данные для демаскировки посредством обработки содержащихся в денежном запросе данных для изготовления вслепую денежной подписи денежным секретным ключом, соответствующим сумме кредитования целевого платежного сертификата, и доставляют их плательщику, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, и принимают их в качестве данных для получения подписи целевого платежного сертификата, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня денежного секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки

RU 2157001 C2

RU 2157001 C2

его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

48. Способ проведения платежей по п.47, отличающийся тем, что при создании основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификата и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

49. Способ проведения платежей по п.47, отличающийся тем, что при включении в основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

50. Способ проведения платежей по любому из пп.47, или 48, или 49, отличающийся тем, что при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

51. Способ проведения платежей по п.47, отличающийся тем, что перед включением в платежные данные платежного поручения плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

52. Способ проведения платежей по п.47, отличающийся тем, что оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

53. Способ проведения платежей по п.47, отличающийся тем, что в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

54. Способ проведения платежей по п.53, отличающийся тем, что при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

55. Способ проведения платежей по п.54, отличающийся тем, что наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

56. Способ проведения платежей по п.47, отличающийся тем, что получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей подписи, получатель платежа до платежной операции проверяет подпись получателя платежа для данных обязательства получателя платежа перед плательщиком.

57. Способ проведения платежей по п.47, отличающийся тем, что при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

58. Способ проведения платежей по п.47, отличающийся тем, что при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

RU 2157001 C2

RU 2157001 C2

59. Способ проведения платежей по п.47, отличающийся тем, что при открытии платежного счета, связанного с авторизуемым платежным сертификатом, производят его предварительно дебетование.

60. Способ проведения платежей по п.47, отличающийся тем, что при операции пополнения платежного сертификата формирование денежного запроса производят в соответствии с единой для всех денежных запросов структурой.

61. Способ проведения платежей по 47, отличающийся тем, что подпись авторизуемого платежного сертификата изготавливают посредством понижения уровня имеющейся у плательщика подписи платежного сертификата.

62. Способ проведения платежей по любому из пп.47 - 61, отличающийся тем, что при проведении платежной операции в качестве плательщика выступает получатель платежа.

63. Способ проведения платежей по любому из пп.47 - 62, отличающийся тем, что имеется по меньшей мере два платежных сервера оператора платежной системы.

64. Способ проведения платежей, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одну основу платежного сертификата, которая включает его номер, и получает подпись платежного сертификата посредством изготовления вслепую денежной подписи оператором платежной системы, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, причем при проверке платежеспособности используемого при платеже платежного сертификата оператор платежной системы проводит операцию его авторизации, при которой по наличию информации об авторизуемом платежном сертификате в информационном хранилище отказывают в авторизации, а по ее отсутствию осуществляют проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, и в случае правильности заносят информацию об авторизуемом платежном сертификате в информационное хранилище, после чего формируют ответ оператора платежной системы на платежное поручение получателя платежа и доставляют его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, отличающийся тем, что в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи платежного сертификата посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении операции пополнения платежного устройства плательщик дополнительно формирует платежное требование, включающее замаскированную подпись выбранного платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и подписанное одним из секретных ключей подписи плательщика, и доставляют его промежуточному плательщику, который проверяет подпись для платежного требования открытым ключом подписи плательщика, соответствующим использованному секретному ключу подписи плательщика, формирует и доставляет в платежный сервер оператора платежной системы денежный запрос, который включает дополнительно замаскированную промежуточным плательщиком полученную от плательщика замаскированную подпись выбранного платежного сертификата и идентификатор счета промежуточного плательщика, причем денежный запрос подписывают секретным ключом счета промежуточного плательщика, а оператор платежной системы проверяет подпись денежного запроса промежуточного плательщика открытым ключом счета, идентификатор которого содержится в денежном запросе, осуществляет дебетование этого счета, создает при изготовлении вслепую денежной подписи данные для демаскировки, которые доставляют промежуточному плательщику, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, производит их демаскировку, результат которой доставляют плательщику, который изготавливает подпись платежного сертификата демаскировкой полученных от промежуточного плательщика данных для демаскировки, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством

RU 2157001 C2

RU 2157001 C2

коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, в информационное хранилище при авторизации платежного сертификата заносят подписанное платежное поручение плательщика, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

65. Способ проведения платежей по п.64, отличающийся тем, что при создании основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификата и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

66. Способ проведения платежей по п.64, отличающийся тем, что при включении в основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

67. Способ проведения платежей по любому из пп.64, или 65, или 66, отличающийся тем, что при включении в основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата его включают в основу в качестве дополнительного номера.

68. Способ проведения платежей по п.64, отличающийся тем, что перед включением в платежные данные платежного поручения плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

69. Способ проведения платежей по п.64, отличающийся тем, что оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

70. Способ проведения платежей по п.64, отличающийся тем, что в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

71. Способ проведения платежей по п.70, отличающийся тем, что при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

72. Способ проведения платежей по п.71, отличающийся тем, что наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

73. Способ проведения платежей по п.64, отличающийся тем, что получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей подписи, получатель платежа до платежной операции проверяет подпись получателя платежа для данных обязательства получателя платежа перед плательщиком.

74. Способ проведения платежей по п.64, отличающийся тем, что при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по

RU 2157001 C2

RU 2157001 C2

меньшей мере одной платежной операции.

75. Способ проведения платежей по п.64, отличающийся тем, что при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

76. Способ проведения платежей по любому из пп.64 - 75, отличающийся тем, что при проведении платежной операции в качестве плательщика выступает получатель платежа.

77. Способ проведения платежей по любому из пп.64 - 76, отличающийся тем, что имеется по меньшей мере два платежных сервера оператора платежной системы.

78. Способ проведения платежей, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, создании плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик получает подпись платежного сертификата посредством изготовления вслепую денежной подписи оператором платежной системы, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, отличающийся тем, что в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи платежного сертификата посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежным сертификатом, и в случае отсутствия такого счета, открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня денежного секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством перевода со счета промежуточного плательщика, при которой плательщик дополнительно формирует платежное требование, включающее замаскированную подпись выбранного платежного сертификата в качестве данных для изготовления вслепую денежной подписи и подписанное одним из секретных ключей подписи плательщика, и доставляет его промежуточному плательщику, который проверяет подпись для платежного требования открытым ключом подписи плательщика, соответствующим использованному плательщиком секретному ключу подписи, формирует и доставляет в платежный сервер оператора платежной системы денежный запрос, который включает дополнительно замаскированную промежуточным плательщиком полученную от плательщика замаскированную подпись выбранного платежного сертификата и идентификатор счета промежуточного плательщика, причем денежный запрос подписывают секретным ключом счета промежуточного плательщика, а оператор платежной системы проверяет подпись денежного запроса промежуточного плательщика открытым ключом счета, идентификатор которого содержится в денежном запросе, осуществляет дебетование этого счета, создает при изготовлении вслепую денежной подписи данные для демаскировки, которые доставляют промежуточному плательщику, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, производит их демаскировку, результат которой доставляют плательщику, который изготавливает подпись платежного сертификата демаскировкой полученных от промежуточного плательщика данных для демаскировки, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую

RU 2157001 C2

RU 2157001 C2

предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата. причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

79. Способ проведения платежей по п.78, отличающийся тем, что при создании основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификата и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

80. Способ проведения платежей по п.78, отличающийся тем, что при включении в основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентфкатора используют сам открытый ключ подписи платежного сертификата.

81. Способ проведения платежей по любому из пп.78, или 79, или 80, отличающийся тем, что при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

82. Способ проведения платежей по п.78, отличающийся тем, что перед включением в платежные данные платежного поручения плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

83. Способ проведения платежей по п.78, отличающийся тем, что оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

84. Способ проведения платежей по п.78, отличающийся тем, что в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

85. Способ проведения платежей по п.84, отличающийся тем, что при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

86. Способ проведения платежей по п.85, отличающийся тем, что наперед заданную маскирующую функцию выбирают

RU 2157001 C2

RU 2157001 C2

произвольно из множества односторонних функций.

87. Способ проведения платежей по п.78, отличающийся тем, что получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей подписи, получатель платежа до платежной операции проверяет подпись получателя платежа для данных обязательства получателя платежа перед плательщиком.

88. Способ проведения платежей по п.78, отличающийся тем, что при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

89. Способ проведения платежей по п.78, отличающийся тем, что при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

90. Способ проведения платежей по п.78, отличающийся тем, что при открытии платежного счета, связанного с авторизуемым платежным сертификатом, производят его предварительное дебетование.

91. Способ проведения платежей по любому из пп.78 - 90, отличающийся тем, что при проведении платежной операции в качестве плательщика выступает получатель платежа.

92. Способ проведения платежей по любому из пп.78 - 91, отличающийся тем, что имеется по меньшей мере два платежных сервера оператора платежной системы.

93. Способ проведения платежей, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, создании плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик получает подпись платежного сертификата посредством изготовления вслепую денежной подписи оператором платежной системы, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, отличающийся тем, что в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительного изготовленного совместно с соответствующим ему секретным ключом подписи платежного сертификата посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежным сертификатом, и в случае отсутствия такого счета открывают его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня денежного секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством перевода со счета промежуточного плательщика, при которой плательщик дополнительно формирует платежное требование, включающее замаскированную подпись выбранного платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и подписанную одним из секретных ключей подписи плательщика, и доставляет его промежуточному плательщику, который проверяет подпись для платежного требования открытым ключом подписи плательщика, соответствующим использованному плательщиком секретному ключу подписи, формирует и доставляет в платежный сервер оператора платежной системы денежный запрос, который включает дополнительно замаскированную промежуточным плательщиком полученную от плательщика замаскированную подпись выбранного платежного сертификата и идентификатор счета промежуточного плательщика, причем денежный запрос подписывают секретным ключом счета промежуточного плательщика, а оператор платежной системы проверяет подпись

RU 2157001 C2

RU 2157001 C2

денежного запроса промежуточного плательщика открытым ключом счета, идентификатор которого содержится в денежном запросе, осуществляет дебетование этого счета, создает при изготовлении вслепую денежной подписи данные для демаскировки, которые доставляют промежуточному плательщику, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, производит их демаскировку, результат которой доставляют плательщику, который изготавливает подпись платежного сертификата демаскировкой полученных от промежуточного плательщика данных для демаскировки, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством операции пополнения платежного сертификата, при которой выбирают платежный сертификат и формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, в качестве которых берут замаскированную подпись платежного сертификата наибольшего уровня, предварительно изготовленную посредством демаскировки данных для получения подписи платежного сертификата, и доставляют его в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования по денежному запросу, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством обработки содержащихся в запросе данных для изготовления вслепую денежной подписи соответствующим сумме кредитования денежным секретным ключом и доставляет их отправителю денежного запроса, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, и принимает их в качестве данных для получения подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика и подпись для этого платежного поручения, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

94. Способ проведения платежей по п.93, отличающийся тем, что при создании основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификата и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

RU 2157001 C2

RU 2157001 C2

95. Способ проведения платежей по п.93, отличающийся тем, что при включении в основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

96. Способ проведения платежей по любому из пп.93, или 94, или 95, отличающийся тем, что при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

97. Способ проведения платежей по п.93, отличающийся тем, что перед включением в платежные данные платежного поручения плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

98. Способ проведения платежей по п.93, отличающийся тем, что оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

99. Способ проведения платежей по п.93, отличающийся тем, что в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

100. Способ проведения платежей по п.99, отличающийся тем, что при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

101. Способ проведения платежей по п.100, отличающийся тем, что наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

102. Способ проведения платежей по п.93, отличающийся тем, что получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей подписи, получатель платежа до платежной операции проверяет подпись получателя платежа для данных обязательства получателя платежа перед плательщиком.

103. Способ проведения платежей по п.93, отличающийся тем, что при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

104. Способ проведения платежей по п.93, отличающийся тем, что при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

105. Способ проведения платежей по п.93, отличающийся тем, что при открытии платежного счета, связанного с авторизуемым платежном сертификатом, производят его предварительное дебетование.

106. Способ проведения платежей по п.93, отличающийся тем, что при операции пополнения платежного сертификата формирование денежного запроса производят в соответствии с единой для всех денежных запросов структурой.

107. Способ проведения платежей по п.93, отличающийся тем, что подпись авторизуемого платежного сертификата изготавливают посредством понижения уровня имеющейся у плательщика подписи платежного сертификата.

108. Способ проведения платежей по любому из пп.93 - 107, отличающийся тем, что при проведении платежной операции в качестве плательщика выступает получатель платежа.

109. Способ проведения платежей по любому из пп.93 - 108, отличающийся тем, что имеется по меньшей мере два платежных сервера оператора платежной системы.

RU 2157001 C2

RU 2157001 C2